THE MANIN CONSTANT OF ELLIPTIC CURVES OVER FUNCTION FIELDS

AMBRUS PÁL

Abstract. We study the p-adic valuation of the values of normalised Hecke eigenforms attached to non-isotrivial elliptic curves defined over function fields of transcendence degree one over finite fields of characteristic p. We derive upper bounds on the smallest attained valuation in terms of the minimal discriminant under a certain assumption on the function field and provide examples to show that our estimates are optimal. As an application of our results we also prove the analogue of the degree conjecture unconditionally for strong Weil curves with square-free conductor defined over function fields satisfying the assumption mentioned above.

1. Introduction

Notation 1.1. Let F denote the function field of $\mathcal{C}$, where the latter is a geometrically connected smooth projective curve defined over the finite field $\mathbb{F}_q$ of characteristic p. Let $\mathbb{A}$ denote the ring of adèles of F and let GL_2 denote the group scheme of invertible two by two matrices. Let E be a non-isotrivial elliptic curve defined over F. Then we may associate a cuspidal automorphic representation of $GL_2(\mathbb{A})$ to E as follows. Let $E_{\overline{F}}$ denote the base change of E to the separable closure $\overline{F}$ of F. For every prime l different from p one may attach to the étale cohomology group $H^1(E_{\overline{F}}, \mathbb{Q}_l(1))$, considered as a representation of the absolute Galois group of F, an irreducible cuspidal automorphic representation ρ_E with trivial central character via the Langlands correspondence. As the notation indicates this representation is independent of the choice of l.

Let V_E denote the irreducible constituent of the space of cuspidal automorphic forms on $GL_2(\mathbb{A})$ which realises the representation ρ_E. Then there is a distinguished element ψ_E of V_E which we will call the normalised Hecke eigenform attached to E. It is characterised by the fact that it is invariant under the action of the Hecke congruence group of level $\mathfrak{n}$, where $\mathfrak{n}$ denotes the conductor of the elliptic curve E, and its leading Fourier coefficient is 1. (For an explanation of these concepts as well as an explicit description of the Hecke eigenform see the following chapter.) By a classical theorem of Harder the automorphic form ψ_E takes only finitely many values. On the other hand it is easy to see that it takes only rational values. Hence there is a unique positive rational number $c(E)$ such that the subgroup of $\mathbb{Q}$ generated by the values of ψ_E is equal to $c(E)\mathbb{Z}$. Then the following holds:

Proposition 1.2. *There is a natural number $m(E)$ such that $c(E) = p^{-m(E)}$.*

It is natural to guess that $m(E)$, which we will call the Manin constant of E, is always zero. Although this hypothesis is frequently made (sometimes implicitly)

[1] *2000 Mathematics Subject Classification.* 11G05 (primary), 11G40, 14F30 (secondary).
Date: January 9, 2010.

in the literature (see for example [20], [21] and [23]) it is actually false. One of the aims of this paper is to exhibit many cases when $m(E)$ is not zero. Because the Manin constant could be non-zero many formulas in the literature have to be corrected to include this non-trivial factor. Hence the latter is a very interesting isogeny invariant of the elliptic curve, therefore it is desirable to compute it, or at least to give upper bounds, in terms of more well-known invariants. This is the other major aim of this paper. (This problem has been already studied by Tan in [28], see Remark 7.9 below). We will also discuss the implication of our results in relation with one of the formulas mentioned above.

Let us formulate now the main results of this paper. For every E as above let Δ_E denote the discriminant of a relatively minimal elliptic surface $\mathcal{E} \to \mathcal{C}$ whose generic fibre is E. Then Δ_E is an effective divisor on the curve $\mathcal{C}$. Moreover let g denote the genus of $\mathcal{C}$ and let d be the positive integer such that $q = p^d$. We will show the following:

Theorem 1.3. *Assume that p does not divide the order of* $\mathrm{Pic}_0(\mathcal{C})(\mathbb{F}_q)$*. Then we have:*

$$m(E) \leq d(\frac{1}{12}\deg(\Delta_E) + g - 1),$$

and the two sides of the inequality above are equal when the elliptic surface $\mathcal{E}$ is ordinary in dimension 2*.*

The condition on $\mathrm{Pic}_0(\mathcal{C})(\mathbb{F}_q)$ in the theorem above is satisfied for example when $\mathcal{C}$ is a rational curve or a supersingular elliptic curve. Moreover the moduli space of smooth projective connected curves of genus g with p-rank zero is a variety of dimension $2g-3$ over $\overline{\mathbb{F}}_p$ when $g \geq 2$ and p is odd (see Theorem 2.3 and Proposition 2.7 of [4] on pages 120 and 122, respectively). Hence there are plenty of curves satisfying this condition. It is natural to expect that most elliptic surfaces are ordinary in dimension 2 (for a precise formulation of this conjecture see Remark 6.12). In particular our estimate in Theorem 1.3 should be the best possible (at least if we want to make one in terms of the discriminant). We can verify the ordinariness condition in many cases. The following result is just a sample of what can be proven with our methods.

Theorem 1.4. *Let p be a prime number and let n be a positive integer such that $n|p-1$ and $6|n$. Let E be the elliptic curve defined over the rational function field $F = \mathbb{F}_p(T)$ by the Weierstrass equation*

$$y^2 + xy = x^3 - T^n.$$

Then E is not isotrivial and

$$m(E) = \frac{n}{6} - 1 = \frac{1}{12}\deg(\Delta_E) - 1.$$

The basic strategy of the proof of Theorem 1.3 is to relate the Manin constant to the p-adic valuation of coefficients of L-functions of E. The key tools in estimating the latter are a mild equivariant extension of Katz's conjecture relating the Newton and Hodge polygons and a theorem of Chinburg computing the refined equivariant Euler characteristic of the de Rham complex of varieties equipped with tame group actions in terms of ϵ-constants. The proof of Theorem 1.4 is closely related. In fact the reason why it is particularly convenient to work with those elliptic curves which appear in the theorem is that Ulmer computed their Hasse-Weil L-functions rather explicitly in [29].

In the rest of the introduction we describe the application of Theorem 1.3 in this paper which was the main motivation for our investigations. Fix a closed point ∞ of $\mathcal{C}$ and assume that E has split multiplicative reduction at ∞. Then $\mathfrak{n} = \mathfrak{m}\infty$ for an effective divisor $\mathfrak{m}$ on $\mathcal{C}$ where we write the addition of divisors multiplicatively in this paper. Let A denote the ring of rational functions on $\mathcal{C}$ regular away from ∞ and let $X_0(\mathfrak{m})$ denote the unique smooth projective curve over F which contains the affine Drinfeld modular curve $Y_0(\mathfrak{m})$ parameterising Drinfeld A-modules of rank two of generic characteristic with Hecke level $\mathfrak{m}$-structure as a dense open subscheme. Then there is a non-trivial map $\pi : X_0(\mathfrak{m}) \to E$ of curves defined over F. We say that E is a strong Weil curve if the modular parameterisation π above can be chosen so that the kernel of the map induced by π via Albanese functoriality is smooth and connected in the Jacobian of $X_0(\mathfrak{m})$. In this case we say that π is optimal. Up to isomorphism there is exactly one strong Weil curve in the isogeny class of E. With the help of Theorem 1.3 and the Pesenti-Szpiro inequality we will show the following

Theorem 1.5. *Assume that p does not divide the order of* $\mathrm{Pic}_0(\mathcal{C})(\mathbb{F}_q)$. *Also suppose that π is optimal and $\mathfrak{m}$ is square-free. Then we have:*

$$\deg(\pi) < q^{18g+4\deg(\infty)+1} \cdot q^{2\deg(\mathfrak{m})} \cdot \deg(\mathfrak{m})^3.$$

The result above is an analogue of Frey's celebrated degree conjecture, formulated originally for strong Weil curves over $\mathbb{Q}$. Our result completes the work of Papikian (see [21]). In his paper he made a conjecture which implies that the Manin constant is zero (at least when F is the rational function field and ∞ is the point at infinity) and he derived an inequality significantly stronger then the one in Theorem 1.5 under this assumption. As we saw his hypothesis does not hold in general. In fact it is quite reasonable to expect in light of the above that $m(E)$ is $d(\frac{1}{12}\deg(\Delta_E) + g - 1)$ when E is minimal in its isogeny class (for the definition of the latter see chapter 7). This is reflected by the fact that the contribution of our estimate of the term $c(E)^{-2}$ to our bound on the degree of the modular parameterisation is significant, it is of the size $O(q^{\deg(\mathfrak{m})})$.

Contents 1.6. In the following chapter we will give an explicit description of the Hecke eigenform and prove Proposition 1.2. In the third chapter we will work out carefully in detail the analogue of the theory of modular symbols for function fields, something which is missing from the current literature. Using these results we derive lower and upper bounds on the Manin constant in terms of the p-adic valuation of coefficients of L-functions of E twisted with tamely ramified abelian characters in the fourth chapter. The aim of the fifth chapter is to relate the Galois module structure of the second coherent cohomology of the structure sheaf of elliptic surfaces equipped with a group action respecting the elliptic fibration to ϵ-constants of Galois representations of the function field of the base in a special case. We prove a mild equivariant extension of Katz's conjecture relating the Newton and Hodge polygons and with its aid we derive Theorem 1.3 from our previous results in the sixth chapter. In the seventh chapter we show that the isogeny class of E contains an elliptic curve whose j-invariant is not a p-th power then we use this result and the Pesenti-Szpiro inequality to deduce a bound on $m(E)$ in terms of the degree of the conductor of E from Theorem 1.3. In the eighth chapter we first review the work of Ulmer in [29] then prove Theorem 1.4 by using the latter and a classical result of Stickelberger on p-adic valuations of Gauss sums. We show that the usual characterisation of strong Weil curves and optimal modular parameterisations holds in the function field setting as well in the ninth chapter. In the last chapter we first show that a certain homomorphism defined by Gekeler and Reversat in [5] has finite cokernel of exponent dividing $q^{\deg(\infty)}-1$. Then we combine this result with the bound in chapter seven and the work of Papikian to show Theorem 1.5.

Acknowledgement 1.7. The author was partially supported by the EPSRC grant P19164.

2. The normalised Hecke eigenform

Notation 2.1. Let $\mathcal{O}$ denote the maximal compact subring of the ring $\mathbb{A}$ of adèles of F. Let $|\mathcal{C}|$ denote the set of closed points of $\mathcal{C}$. For every adèle $a \in \mathbb{A}$ and $x \in |\mathcal{C}|$ let a_x denote the x-th component of a. Let μ, μ^* be Haar measures on the locally compact abelian topological groups $\mathbb{A}$ and $\mathbb{A}^*$, respectively. Also assume that $\mu(\mathcal{O})$ and $\mu^*(\mathcal{O}^*)$ are both equal to 1. Since these measures are left-invariant with respect to the discrete subgroups F^* and F by definition, they induce a measure on $F^*\backslash\mathbb{A}^*$ and $F\backslash\mathbb{A}$, respectively, which will be denoted by the same letter by abuse of notation. For every divisor $\mathfrak{m}$ on $\mathcal{C}$ let $\mathfrak{m}\mathcal{O}$, $\mathbb{K}_0(\mathfrak{m})$ denote the sub $\mathcal{O}$-module of $\mathbb{A}$ generated by those idèles whose divisor is $\mathfrak{m}$, and the Hecke congruence subgroup of $GL_2(\mathbb{A})$ of level $\mathfrak{m}$:

$$\mathbb{K}_0(\mathfrak{m}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathcal{O}) | c \in \mathfrak{m}\mathcal{O}\},$$

respectively. Let $\tau : F\backslash\mathbb{A} \to \mathbb{C}^*$ be a non-trivial continuous additive character. The composition of the quotient map $\mathbb{A} \to F\backslash\mathbb{A}$ and τ will be denoted by the same symbol by the usual abuse of notation. Let $\mathcal{D}$ denote the $\mathcal{O}$-module $\mathcal{D} = \{x \in \mathbb{A} | \tau(x\mathcal{O}) = 1\}$, and let $\mathfrak{d}$ be a divisor on $\mathcal{C}$ such that $\mathcal{D} = \mathfrak{d}\mathcal{O}$. Let $\mathfrak{n}$ be the conductor of E. The latter is an effective divisor on $\mathcal{C}$. We may assume that the divisor $\mathfrak{d}$ is relatively prime to $\mathfrak{n}$ by changing τ, if necessary. Let B denote the group scheme of invertible upper triangular two by two matrices. Let P denote the group scheme of invertible upper triangular two by two matrices with 1 on the lower right corner. Finally let Z denote the centre of the group scheme GL_2.

Definition 2.2. For every idèle $u \in \mathbb{A}^*$ let (u) denote the corresponding divisor on $\mathcal{C}$. Often we will denote (u) simply by u by slight abuse of notation, when this does not cause confusion. We will call two divisors $\mathfrak{m}$ and $\mathfrak{n}$ on $\mathcal{C}$ relatively prime if their support is disjoint. Let $\mathrm{Div}(\mathcal{C})$ denote the group of divisors on $\mathcal{C}$. We will call a function $f : \mathrm{Div}(\mathcal{C}) \to \mathbb{C}$ multiplicative if it vanishes on non-effective divisors, $f(1) = 1$ and for every pair of relatively prime divisors $\mathfrak{n}$ and $\mathfrak{m}$ we have $f(\mathfrak{n}\mathfrak{m}) = f(\mathfrak{n})f(\mathfrak{m})$. Let E be a non-isotrivial elliptic curve defined over $\mathcal{C}$ of conductor $\mathfrak{n}$. For every divisor $\mathfrak{r}$ on $\mathcal{C}$ let $\deg(\mathfrak{r})$ denote the degree of $\mathfrak{r}$. For every $x \in |\mathcal{C}|$ let $L_x(E,t)$ denote the local factor of the Hasse-Weil L-function of E at x. The latter can be written in the form:

$$L_x(E,t) = \sum_{n=0}^{\infty} a(x^n)(tq)^{n\deg(x)} \in \mathbb{Z}[[t]],$$

for some $a(x^n) \in \mathbb{Z}[\frac{1}{p}]$. Let a denote the unique multiplicative function into the multiplicative semigroup of $\mathbb{Q}$ such that $a(x^n)$ is the same as above for each natural number n and each $x \in |\mathcal{C}|$. A continuous function $\psi_E : GL_2(\mathbb{A}) \to \mathbb{Q}$ is called a normalised Hecke eigenform attached to E is if it satisfies the following properties:

(a) it is automorphic: $\psi_E(\gamma h)=\psi_E(h)$ for all $\gamma\in GL_2(F)$,
(b) it has trivial central character: $\psi_E(hz)=\psi_E(h)$ for all $z\in Z(\mathbb{A})$,
(c) it is right $\mathbb{K}_0(\mathfrak{n})$-invariant: $\psi_E(hk)=\psi_E(h)$ for all $k\in\mathbb{K}_0(\mathfrak{n})$,
(d) it is cuspidal:

$$\int_{F\backslash\mathbb{A}}\psi_E(\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}h)d\mu(x)=0\text{ for all }h\in GL_2(\mathbb{A}),$$

(e) its Fourier coefficients are a:

$$a(\mathfrak{m}\mathfrak{d})=\mu(F\backslash\mathbb{A})^{-1}\int_{F\backslash\mathbb{A}}\psi_E(\begin{pmatrix}\overline{\mathfrak{m}} & x\\ 0 & 1\end{pmatrix})\tau(-x)d\mu(x)\text{ for all }\mathfrak{m}\in\text{Div}(\mathcal{C}),$$

where $\overline{\mathfrak{m}}\in\mathbb{A}^*$ and $(\overline{\mathfrak{m}})=\mathfrak{m}$.

Note that the last two conditions make sense because of (a) we may (and will) consider ψ_E as a function on $GL_2(F)\backslash GL_2(\mathbb{A})$ as well.

Proposition 2.3. *There is a unique normalised Hecke eigenform attached to E.*

The claim above is certainly very well known and the only fact which needs an additional argument is that ψ_E takes only rational values. As we will shortly prove a stronger claim we will omit the proof. By a classical theorem of Harder (see [7]) the normalised Hecke eigenform ψ_E is supported on a finite set as a function on the double coset $GL_2(F)\backslash GL_2(\mathbb{A})/\mathbb{K}_0(\mathfrak{n})Z(\mathbb{A})$. Let $L(E)\subseteq\mathbb{Q}$ denote the $\mathbb{Z}$-module generated by the values of ψ_E. By the above there is a unique positive rational number $c(E)\in\mathbb{Q}$ such that $L(E)=c(E)\mathbb{Z}$.

Proposition 2.4. *There is a non-negative natural number $m(E)$ such that $c(E)=p^{-m(E)}$.*

As we already mentioned in the introduction we will call $m(E)$ the Manin constant of the elliptic curve E.

Proof. First we are going to show that $L(E)\subseteq\mathbb{Z}[\frac{1}{p}]$. By the approximation theorem we have $GL_2(\mathbb{A})=GL_2(F)P(\mathbb{A})Z(\mathbb{A})\mathbb{K}_0(\mathfrak{n})$. Therefore it will be sufficient to prove that $\psi_E(h)\in\mathbb{Z}[\frac{1}{p}]$ for every element h of $P(\mathbb{A})$. By the definition of Fourier coefficients:

$$\psi_E(\begin{pmatrix}y & x\\ 0 & 1\end{pmatrix})=\sum_{\eta\in F^*}a(\eta y\mathfrak{d}^{-1})\tau(\eta x)=\sum_{\eta\in S}a(\eta y\mathfrak{d}^{-1})(\sum_{\epsilon\in\mathbb{F}_q^*}\tau(\eta\epsilon x))$$

for all $y\in\mathbb{A}^*$, $x\in\mathbb{A}$, where S is a set of representatives of the quotient $\mathbb{F}_q^*\backslash F^*$, since ψ_E is cuspidal. The character sums on the right hand side are all equal to -1 or $q-1$. Moreover the sum above is finite. As $a(\mathfrak{m})\in\mathbb{Z}[\frac{1}{p}]$ for every effective divisor $\mathfrak{m}$, the claim is now clear. Now we only need to show that $-1\in L(E)$ in order to prove the proposition. Let $\overline{\mathfrak{d}}\in\mathbb{A}^*$ be such that $(\overline{\mathfrak{d}})=\mathfrak{d}$. Then the Fourier expansion says:

$$\psi_E(\begin{pmatrix}\overline{\mathfrak{d}} & x\\ 0 & 1\end{pmatrix})=\sum_{\eta\in F^*}a(\eta)\tau(\eta x)=\sum_{\epsilon\in\mathbb{F}_q^*}a(\epsilon)\tau(\epsilon x)=\sum_{\epsilon\in\mathbb{F}_q^*}\tau(\epsilon x),$$

because $F^*\cap\mathcal{O}=\mathbb{F}_q^*$ and $a(1)=1$ by definition. The character sum on the right hand side is equal to -1 if $x\notin\mathcal{D}$. □

3. Epsilon constants and toric integrals

Notation 3.1. For the rest of the paper fix a prime number l different from p. By the axiom of choice we may pick an isomorphism $\iota : \overline{\mathbb{Q}}_l \to \mathbb{C}$. We will identify $\overline{\mathbb{Q}}_l$ with $\mathbb{C}$ via ι in all that follows. Let E_l be a finite extension of $\mathbb{Q}_l$ and let $\rho : \mathrm{Gal}(\overline{F}|F) \to GL_{E_l}(W)$ be an l-adic representation on a finite dimensional vector space W over E_l. Moreover let $L(\rho, t) \in E_l[[t]]$ denote the Grothendieck L-function associated to ρ as defined in 9.1 of [2] on page 574. By a classical theorem of Grothendieck (§10 of [2] on pages 581-592) the series $L(\rho, t)$ is a rational function in the variable t and also satisfies the functional equation:

$$L(\rho, t) = \epsilon(\rho) t^{\alpha(\rho)} L(\rho^\vee, q^{-1}t^{-1})$$

where $\alpha(\rho) \in \mathbb{Z}$, $\epsilon(\rho) \in E_l^*$ and $\rho^\vee$ is the degree of the conductor of ρ (in the sense of [13], page 179), the ϵ-constant of ρ, and the dual l-adic representation on $\mathrm{Hom}(W, E_l)$, respectively.

Notation 3.2. Let K be a local field, let dx be a Haar measure on K, and let ψ be a non-trivial additive character on K. For every continuous homomorphism $\alpha : K^* \to \mathbb{C}^*$ let $\epsilon(K, \alpha, \psi, dx)$ denote the local ϵ-factor attached to the triple (α, ψ, dx) as defined in 3.3 of [2] on page 526. Let $W(\overline{K}|K) < \mathrm{Gal}(\overline{K}|K)$ denote the Weil group of K (as defined in 2.2.4 of [2] on page 522). Local class field theory furnishes an isomorphism $j : K^* \to W(\overline{K}|K)^{ab}$. We normalise this isomorphism so that for every uniformizer $\pi \in K^*$ the image of $j(\pi)$ with respect to the map $W(\overline{K}|K) \to \mathbb{Z}$ introduced in 2.2.4 of [2] is the geometric Frobenius (similarly to 2.3 of [2] on page 523). For every homomorphism $\alpha : \mathrm{Gal}(\overline{K}|K) \to \mathbb{C}^*$ let the same symbol α denote the composition of j, considered here as an imbedding $j : K^* \to \mathrm{Gal}(\overline{K}|K)^{ab}$, with the map $\mathrm{Gal}(\overline{K}|K)^{ab} \to \mathbb{C}^*$ induced by the character α by slight abuse of notation.

Notation 3.3. For every $x \in |\mathcal{C}|$ let F_x, $\mathcal{O}_x$ denote the completion of F at x and the valuation ring of F_x, respectively. For every $x \in |\mathcal{C}|$ let μ_x, μ_x^* be the unique Haar measures on the locally compact abelian topological groups F_x and F_x^*, respectively, so that $\mu(\mathcal{O}_x)$ and $\mu^*(\mathcal{O}_x^*)$ are both equal to 1. Moreover for every $x \in |\mathcal{C}|$ let $\tau_x : F_x \to \mathbb{C}^*$ be the unique continuous additive character such that $\tau(a) = \prod_{x \in |\mathcal{C}|} \tau_x(a_x)$ for every $a \in \mathbb{A}$. For every homomorphism $\alpha : \mathrm{Gal}(\overline{F}|F) \to \mathbb{C}^*$ and for every $x \in |\mathcal{C}|$ let $\alpha_x : \mathrm{Gal}(\overline{F}_x|F) \to \mathbb{C}^*$ denote the restriction of α onto the decomposition group at x.

Theorem 3.4. *For every continuous homomorphism* $\alpha : \mathrm{Gal}(\overline{K}|K) \to \mathbb{C}^*$ *with finite image we have:*

$$\epsilon(\alpha) = q^{1-g} \prod_{x \in |\mathcal{C}|} \epsilon(F_x, \alpha_x, \tau_x, \mu_x).$$

Proof. This is just a special case of Théorème 3.2.1.1 of [13] on page 187. □

Definition 3.5. For every divisor $\mathfrak{m}$ on $\mathcal{C}$ let $\underline{\mathfrak{m}}$ denote the support of $\mathfrak{m}$. Let $c \in \mathbb{A}^*$ be an idèle so that $\mathfrak{c} = (c)$ is an effective divisor on $\mathcal{C}$. For every such c let $\widehat{c} \in \mathbb{A}$ be the unique adèle such that $\widehat{c}_x = c_x^{-1}$ for every $x \in \underline{\mathfrak{c}}$, and $\widehat{c}_x = 0$, otherwise. Let $\alpha : F\backslash\mathbb{A}^* \to \mathbb{C}^*$ be a continuous character with finite image whose conductor $\mathfrak{c}'$ divides $\mathfrak{c}$. For every $z \in \mathbb{C}$ let $I(\psi_E, \mathfrak{c}, \alpha, z)$ denote the integral:

$$I(\psi_E, \mathfrak{c}, \alpha, z) = \int_{F^*\backslash\mathbb{A}^*} \psi_E(\begin{pmatrix} y & y\widehat{c} \\ 0 & 1 \end{pmatrix}) \alpha(y) z^{\deg(y)} d\mu^*(y) \in \mathbb{C}.$$

Lemma 3.6. *The integral $I(\psi_E,\mathfrak{c},\alpha,z)$ is well-defined and it is independent of the choice of c as the notation indicates.*

Proof. By Lemma 2 of [28] on pages 300-301 the integrand of $I(\psi_E,\mathfrak{c},\alpha,z)$ is compactly supported. Hence the latter is well-defined. Choose another idèle $c'\in\mathbb{A}^*$ such that $(c')=\mathfrak{c}$. Then there is an $u\in\mathcal{O}^*$ such that $c'=uc$ and therefore $\widehat{c}'=u\widehat{c}$. Now the claim follows from the $GL_2(\mathcal{O})$-invariance of ψ_E. □

Notation 3.7. Let $W(\overline{F}|F)<\mathrm{Gal}(\overline{F}|F)$ denote the Weil group of F (as defined in 2.4 of [2] on page 524). Global class field theory furnishes an isomorphism $\mathbf{j}:F^*\backslash\mathbb{A}^*\to W(\overline{F}|F)^{ab}$ which is compatible with the isomorphism between F_x^* and $W(\overline{F}_x|F_x)^{ab}$ introduced in Notation 3.2 for every $x\in|\mathcal{C}|$ (in the sense of 2.4 of [2] on page 525). For every homomorphism $\alpha:\mathrm{Gal}(\overline{F}|F)\to\mathbb{C}^*$ let the same symbol α denote the composition of $\mathbf{j}$, considered here as an imbedding $\mathbf{j}:F^*\backslash\mathbb{A}^*\to\mathrm{Gal}(\overline{F}|F)^{ab}$, with the map $\mathrm{Gal}(\overline{F}|F)^{ab}\to\mathbb{C}^*$ induced by the character α. Moreover let α also denote the composition of the quotient map $\mathbb{A}^*\to F^*\backslash\mathbb{A}^*$ and the map $\alpha:F^*\backslash\mathbb{A}^*\to\mathbb{C}^*$ introduced above by the usual abuse of notation.

Notation 3.8. For every divisor $\mathfrak{m}$ on $\mathcal{C}$ relatively prime to $\mathfrak{c}$ and for every $\overline{\mathfrak{m}}\in\mathbb{A}^*$ such that $(\overline{\mathfrak{m}})=\mathfrak{m}$ the complex number $\alpha(\overline{\mathfrak{m}})$ is independent of the choice of $\overline{\mathfrak{m}}$. We let $\alpha(\mathfrak{m})$ denote this common value. Let σ_E denote the natural l-adic representation of $\mathrm{Gal}(\overline{F}|F)$ on the cohomology group $H^1(E_{\overline{F}},\mathbb{Q}_l)$. By definition $L(E,t)=L(\sigma_E,t)$. The twisted L-function $L(\sigma_E\otimes\alpha,t)$ is actually a polynomial in the variable t and therefore it can be evaluated at any complex number $t=z$. Finally let $G(E,\alpha,\mathfrak{c},,t)\in\mathbb{C}[t]$ denote the polynomial:

$$G(E,\alpha,\mathfrak{c},t)=\prod_{x\in\underline{\mathfrak{c}}-\underline{\mathfrak{c}}'}\big(-1+a(x)\alpha(x)(qt)^{\deg(x)}-\alpha(x)^2t^{2\deg(x)}\big).$$

Proposition 3.9. *Assume that $\mathfrak{c}$ is square-free and it is relatively prime to $\mathfrak{d}\mathfrak{n}$. Then the following holds:*

$$I(\psi_E,\mathfrak{c},\alpha,z)=\alpha(\mathfrak{d}^2\mathfrak{c}')\epsilon(\alpha^{-1})\prod_{x\in\underline{\mathfrak{c}}}(q^{\deg(x)}-1)^{-1}\left(\frac{z^2}{q}\right)^{g-1}G(E,\alpha,\mathfrak{c},z)L(\sigma_E\otimes\alpha,zq^{-1}).$$

Proof. According to the Fourier expansion of ψ_E we have:

$$\psi_E(\begin{pmatrix}y & y\widehat{c}\\ 0 & 1\end{pmatrix})=\sum_{\eta\in F^*}a(\eta y\mathfrak{d}^{-1})\tau(\eta y\widehat{c}),$$

for every $y\in\mathbb{A}^*$ and the sum on the right is finite. If we interchange this summation and the integration we get:

$$I(\psi_E,\mathfrak{c},\alpha,q^{-s})=\int_{\mathbb{A}^*}a(y\mathfrak{d}^{-1})\tau(y\widehat{c})\alpha(y)q^{-s\deg(y)}d\mu^*(y) \tag{3.9.1}$$

for every $s\in\mathbb{C}$. This computation is justified by Lebesgue's convergence theorem if the second integral is absolutely convergent. But the latter holds if $\mathrm{Re}(s)>1/2$ as the function $y\mapsto a(y\mathfrak{d}^{-1})$ has support on $\mathfrak{d}^{-1}\mathcal{O}$ and

$$|a(y\mathfrak{d}^{-1})\tau(y\widehat{c})|=|a(y\mathfrak{d}^{-1})|\leq 2q^{-1/2\deg(y\mathfrak{d}^{-1})}$$

by the Weil conjectures.

Let $\mathbb{A}_{\mathfrak{c}}$ and $\mathcal{O}_{\mathfrak{c}}$ denote the restricted direct products $\prod'_{x\notin\underline{\mathfrak{c}}}F_x$ and $\prod'_{x\notin\underline{\mathfrak{c}}}\mathcal{O}_x$, respectively. Then $\mathbb{A}_{\mathfrak{c}}$ is a locally compact topological ring and $\mathcal{O}_{\mathfrak{c}}$ is its maximal compact subring. Let $\nu^*_{\mathfrak{c}}$ be a Haar measure on $\mathbb{A}^*_{\mathfrak{c}}$ such that $\nu^*_{\mathfrak{c}}(\mathcal{O}^*_{\mathfrak{c}})$ is equal to 1. Let $|\cdot|_x$ be the absolute value on F_x normalised so that $\mu_x(t\mathcal{O})=|t|_x$ for every $y\in F_x$. Using Fubini's theorem the integral (3.9.1) can be rewritten as

$$\int_{\mathbb{A}^*_{\mathfrak{c}}} a(y\mathfrak{d}^{-1})\alpha(y)q^{-s\deg(y)}d\nu^*_{\mathfrak{c}}(y)\cdot\prod_{x\in\underline{\mathfrak{c}}}\int_{F^*_x} a(t)\tau_x(tc_x^{-1})\alpha_x(t)|t|^s_x d\mu^*_x(t). \tag{3.9.2}$$

The integrand of the first integral of (3.9.2) is invariant under multiplication by $\mathcal{O}^*_{\mathfrak{c}}$. Therefore it is equal to

$$\sum_{\substack{\mathfrak{m}\in\mathrm{Div}(\mathcal{C})\\ \underline{\mathfrak{m}}\cap\underline{\mathfrak{c}}=\emptyset}} a(\mathfrak{m})\alpha(\mathfrak{m}\mathfrak{d})q^{-s\deg(\mathfrak{m}\mathfrak{d})}=\alpha(\mathfrak{d})q^{-s\deg(\mathfrak{d})}\cdot\prod_{x\notin\underline{\mathfrak{c}}}L_x(\sigma_E\otimes\alpha,q^{-(s+1)}). \tag{3.9.3}$$

For every $x\in\underline{\mathfrak{c}}$ the corresponding term in the product (3.9.2) can be rewritten as

$$\int_{F^*_x} a(t)\tau_x(tc_x^{-1})\alpha_x(t)|t|^s_x d\mu^*_x(t)= \\ \sum_{n=0}^{\infty} a(x^n)\alpha_x(c_x)^n|c_x|^{ns}_x\int_{\mathcal{O}^*_x}\tau_x(tc_x^{n-1})\alpha_x(t)d\mu^*_x(t) \tag{3.9.4}$$

because $c_x\in F^*_x$ is a uniformizer, and $a(x^n)=0$ if $n<0$. Suppose now that x divides the conductor of α. Then the restriction of α_x onto $\mathcal{O}^*_x$ is a non-trivial character, therefore

$$\int_{\mathcal{O}^*_x}\tau_x(tc_x^{n-1})\alpha_x(t)d\mu^*_x(t)=\begin{cases}\frac{\alpha_x(c_x)}{q^{\deg(x)}-1}\epsilon(F_x,\alpha_x^{-1},\tau_x,\mu_x), & \text{if } n=0,\\ 0, & \text{otherwise,}\end{cases} \tag{3.9.5}$$

by (3.4.3.2) of [2] on page 528, where we also used the fact that the additive character τ_x restricted to $\mathcal{O}_x$ is trivial. Hence we get

$$\int_{F^*_x} a(t)\tau_x(tc_x^{-1})\alpha_x(t)|t|^s_x d\mu^*_x(t)=\frac{\alpha_x(c_x)}{q^{\deg(x)}-1}\epsilon(F_x,\alpha_x^{-1},\tau_x,\mu_x) \tag{3.9.6}$$

in this case. Otherwise the restriction of α_x onto $\mathcal{O}^*_v$ is the trivial character therefore the left hand side of (3.9.4) is equal to

$$\frac{-1}{q^{\deg(x)}-1}+\sum_{n=1}^{\infty}a(x^n)\alpha_x(c_x)^n|c_x|^{ns}_x=L_x(\sigma_E\otimes\alpha,q^{-(s+1)})-\frac{q^{\deg(x)}}{q^{\deg(x)}-1}. \tag{3.9.7}$$

Because both σ_E and α are unramified at x we have:

$$L_x(\sigma_E\otimes\alpha,q^{-(s+1)})=\big(1-a(x)\alpha(x)q^{-s\deg(x)}+\alpha(x)^2q^{-(2s+1)\deg(x)}\big)^{-1}. \tag{3.9.8}$$

Hence we get that

$$\int_{F^*_x} a(t)\tau_x(tc_x^{-1})\alpha_x(t)|t|^s_x d\mu^*_x(t)= \\ \frac{1}{q^{\deg(x)}-1}\big(-1+a(x)\alpha(x)q^{(1-s)\deg(x)}-\alpha(x)^2q^{-2s\deg(x)}\big)\cdot L_x(\sigma_E\otimes\alpha,q^{-(s+1)}) \tag{3.9.9}$$

in this case. By Theorem 3.4 we have:

$$\epsilon(\alpha^{-1})=q^{1-g}\alpha^{-1}(\mathfrak{d})q^{\deg(\mathfrak{d})}\prod_{x\in\underline{\mathfrak{c}}'}\epsilon(F_x,\alpha_x^{-1},\tau_x,\mu_x) \tag{3.9.10}$$

because according to (3.4.3.1) of [2] on page 528 we have:

$$\epsilon(F_x,\alpha_x^{-1},\tau_x,\mu_x)=\alpha_x^{-1}(\mathfrak{d}_x)q^{\deg(\mathfrak{d}_x)}$$

if α_x is unramified, since we assumed that $\mu_x(\mathcal{O}_x) = 1$ and $\mathfrak{c}$ and $\mathfrak{d}$ are relatively prime. Combining (3.9.3), (3.9.6), (3.9.9) and (3.9.10) we get:

$$\begin{aligned} I(\psi_E, \mathfrak{c}, \alpha, q^{-s}) = \alpha(\mathfrak{d}^2\mathfrak{c}')\epsilon(\alpha^{-1})q^{g-1-(s+1)\deg(\mathfrak{d})}\prod_{x\in\underline{\mathfrak{c}}}(q^{\deg(x)}-1)^{-1} \\ \cdot G(E,\alpha,\mathfrak{c},q^{-s})L(\sigma_E\otimes\alpha, q^{-(s+1)}), \end{aligned} \tag{3.9.11}$$

if we also use that $L_x(\sigma_E \otimes \alpha, q^{-(s+1)}) = 1$ when $x \in \underline{\mathfrak{c}}'$. Because $\deg(\mathfrak{d}) = 2g-2$ the claim now follows for every complex number q^{-s} such that $\mathrm{Re}(s) > 1/2$. But both sides of the equation in the proposition above are polynomials in z hence the claim must hold for every complex number as well. □

4. Lower and upper bounds

Notation 4.1. For every field K let $\overline{K}$ denote a separable closure of K. Let $v_q : \overline{\mathbb{Q}}_p^* \to \mathbb{Q}$ denote the p-adic valuation normalised such that $v_q(q) = 1$. Every polynomial $P(t) \in \overline{\mathbb{Q}}_p[t]$ can be written in the form:

$$P(t) = at^k \prod_{i=1}^{n-k}(1-\lambda_i t), \quad a \in \overline{\mathbb{Q}}_p^*, \quad \lambda_i \in \overline{\mathbb{Q}}_p,$$

where the λ_i are the reciprocal roots of $P(t)$. Let $l_q(P(t)) \in \mathbb{Q}$ denote the non-negative number:

$$l_q(P(t)) = \sum_{v_q(\lambda_i)\leq 1}(1-v_q(\lambda_i)).$$

Let $\mu_\infty, \mu_{\infty,p} \subset \overline{\mathbb{Q}}_p^*$ denote the subgroup of roots of unity and roots of unity whose order is prime to p, respectively.

Lemma 4.2. *With the same notation as above the following holds:*

$$\min_{\epsilon\in\mu_\infty}(v_q(P(\epsilon q^{-1}))) = v_q(a) - k - l_q(P(t)).$$

Moreover the minimum is attained at all but finitely many $\epsilon \in \mu_{\infty,p}$.

Proof. For a fixed $i = 1, 2, \ldots, k$ and for every $\epsilon \in \mu_\infty$ we have:

$$v_q(1-\lambda_i\epsilon q^{-1}) = -1 + v_q(\lambda_i - \epsilon^{-1}q) \geq \min\{0, v_q(\lambda_i) - 1\},$$

so for all but finitely many $\epsilon \in \mu_{\infty,p}$ we have:

$$v_q(1-\lambda_i\epsilon q^{-1}) = \min\{0, v_q(\lambda_i) - 1\}.$$

Therefore for all but finitely many $\epsilon \in \mu_{\infty,p}$ we have:

$$v_q(P(\epsilon q^{-1})) = \min_{\zeta\in\mu_\infty}(v_q(P(\zeta q^{-1}))) = v_q(a) - k + \sum_{i=1}^{\deg(P)}\min\{0, v_q(\lambda_i)-1\}.$$

□

Let $\mathfrak{c}$ be a square-free effective divisor on $\mathcal{C}$ which is relatively prime to $\mathfrak{d}\mathfrak{n}$. Let $\alpha : F\backslash\mathbb{A}^* \to \mathbb{C}^*$ be a continuous character with finite image whose conductor $\mathfrak{c}'$ divides $\mathfrak{c}$.

Lemma 4.3. *The following holds:*

$$\min_{\epsilon\in\mu_\infty}(v_q(G(E,\alpha,\mathfrak{c},\epsilon)))=0.$$

Moreover the minimum is attained at all but finitely many $\epsilon\in\mu_{\infty,p}$.

Proof. For every $x\in\underline{\mathfrak{c}}-\underline{\mathfrak{c}}'$ we have $q^{\deg(x)}a(x)\in\mathbb{Z}$. Hence for every $\epsilon\in\mu_\infty$ and x as above we have:

$$v_q(-1+a(x)\alpha(x)q^{\deg(x)}\epsilon^{\deg(x)}-\alpha(x)^2\epsilon^{2\deg(x)})\geq 0,$$

and for all but finitely many $\epsilon\in\mu_{\infty,p}$ the left hand side is equal to 0. The claim follows by taking the product over all $x\in\underline{\mathfrak{c}}-\underline{\mathfrak{c}}'$. □ □

Lemma 4.4. *For every $y\in\mathbb{A}^*$ and $x\in\mathbb{A}$ there are $\eta\in F$, $u\in\mathcal{O}$ and $c\in\mathbb{A}^*$ such that (c) is a square-free effective divisor which is relatively prime to $\mathfrak{n}$ and*

$$x+u+y^{-1}\eta=\widehat{c}.$$

Proof. Let $z\in\mathbb{A}^*$ be the unique idèle such that for every $v\in|\mathcal{C}|$ we have $z_v=x_v^{-1}$, if $x_v\notin\mathcal{O}_v$, and $z_v=1$, otherwise. Then $\mathfrak{z}=(z)$ is an effective divisor. Let $\mathfrak{y}$ denote the divisor of y^{-1} and let $\mathfrak{b}$ be a square-free effective divisor whose degree is at least $2g-1-\deg(\mathfrak{y})$ and which is relatively prime to $\mathfrak{n}\mathfrak{z}$. Let Z denote the closed scheme of $\mathcal{C}$ whose sheaf of ideals is $\mathcal{O}_{\mathcal{C}}(\mathfrak{z})^\vee\subseteq\mathcal{O}_{\mathcal{C}}$ where for every vector bundle $\mathcal{F}$ on $\mathcal{C}$ we let $\mathcal{F}^\vee$ denote the dual of $\mathcal{F}$. We have an exact sequence

$$H^0(\mathcal{C},\mathcal{O}_{\mathcal{C}}(\mathfrak{y}\mathfrak{b}))\longrightarrow H^0(\mathcal{C},\mathcal{O}_{\mathcal{C}}(\mathfrak{z}\mathfrak{y}\mathfrak{b}))\xrightarrow{i_Z}H^0(Z,\mathcal{O}_{\mathcal{C}}(\mathfrak{z}\mathfrak{y}\mathfrak{b})|_Z)$$

where the first map is induced by the inclusion $\mathcal{O}_{\mathcal{C}}(\mathfrak{y}\mathfrak{b})\subset\mathcal{O}_{\mathcal{C}}(\mathfrak{z}\mathfrak{y}\mathfrak{b})$ and the second map i_Z is the restriction map. By the Riemann-Roch theorem for curves:

$$\dim_{\mathbb{F}_q}H^0(\mathcal{C},\mathcal{F})=2-2g+\deg(\mathcal{F})$$

for every line bundle $\mathcal{F}$ on $\mathcal{C}$ whose degree is at least $2g-1$. Comparing the dimensions of $H^0(\mathcal{C},\mathcal{O}_{\mathcal{C}}(\mathfrak{y}\mathfrak{b}))$ and $H^0(\mathcal{C},\mathcal{O}_{\mathcal{C}}(\mathfrak{z}\mathfrak{y}\mathfrak{b}))$ we get that the image of i_Z has dimension $\deg(\mathfrak{z})$ over $\mathbb{F}_q$. But the dimension of $H^0(Z,\mathcal{O}_{\mathcal{C}}(\mathfrak{z}\mathfrak{y}\mathfrak{b})|_Z)$ is the same hence i_Z is surjective.

Let $b\in\mathbb{A}^*$ be an idèle such that $(b)=\mathfrak{b}$ and $b_v=1$ for every $v\notin\underline{\mathfrak{b}}$. Recall that for every idèle $t\in\mathbb{A}^*$ we have: $H^0(\mathcal{C},\mathcal{O}_{\mathcal{C}}(t))=F\cap t^{-1}\mathcal{O}$. Moreover for every such t we have: $H^0(Z,\mathcal{O}_{\mathcal{C}}(t\mathfrak{z})|_Z)=(tz)^{-1}\mathcal{O}/t^{-1}\mathcal{O}$. Under these identifications i_Z is the composition of the inclusion $F\cap(zb)^{-1}y\mathcal{O}\to(zb)^{-1}y\mathcal{O}$ and the reduction map: $(zb)^{-1}y\mathcal{O}\to(zb)^{-1}y\mathcal{O}/b^{-1}y\mathcal{O}$. Therefore by the above there is an $\eta\in F$ such that for every $v\in|\mathcal{C}|$ we have: $(zby^{-1}\eta)_v\in-1+z_v\mathcal{O}_v$, if $v\in\underline{\mathfrak{z}}$, and $(zy^{-1}b\eta)_v=(y^{-1}b\eta)_v\in\mathcal{O}_v$, otherwise. Because $\mathfrak{b}$ is relatively prime to $\mathfrak{z}$ we get that $(y^{-1}\eta)_v\in-x_v+\mathcal{O}_v$, if $v\in\underline{\mathfrak{z}}$. Let $c\in\mathbb{A}^*$ be the unique idèle such that $c_v=(y\eta^{-1})_v$, if $v\notin\underline{\mathfrak{z}}$ and $(y^{-1}\eta)_v\notin\mathcal{O}_v$, and $c_v=1$, otherwise. By the above (c) divides $\mathfrak{b}$ so it is a square-free effective divisor relatively prime to $\mathfrak{n}$. Let $u=-x-y^{-1}\eta+\widehat{c}$. By the above $u\in\mathcal{O}$ so this choice of η, c and u satisfies the requirements of the claim. □

Let $\mathbb{X}(\mathfrak{n})$ denote the set of tamely ramified continuous characters $F\backslash\mathbb{A}^*\to\mathbb{C}^*$ with finite image whose conductor is relatively prime to $\mathfrak{n}$.

Proposition 4.5. *The following holds:*

$$m(E)\geq d\cdot\sup_{\alpha\in\mathbb{X}(\mathfrak{n})}\big(l_q(L(\sigma_E\otimes\alpha,t))+g-1-v_q(\epsilon(\alpha^{-1}))\big).$$

When p does not divide the order of $\mathrm{Pic}_0(\mathcal{C})(\mathbb{F}_q)$ *the two sides above are actually equal.*

Proof. Fix an isomorphism $\overline{\mathbb{Q}}_p \cong \mathbb{C}$ and let $\alpha \in \mathbb{X}(\mathfrak{n})$ have conductor $\mathfrak{c}$. Without the loss of generality we may assume that $\mathfrak{c}$ is relatively prime to $\mathfrak{d}$ by changing τ, if necessary. According to Proposition 3.9 we have:

$$(4.5.1)\ \ I(\psi_E, \mathfrak{c}, \alpha, z) = \alpha(\mathfrak{d}^2\mathfrak{c}')\epsilon(\alpha^{-1}) \prod_{x \in \underline{\mathfrak{c}}} (q^{\deg(x)} - 1)^{-1}(z^2/q)^{g-1} L(\sigma_E \otimes \alpha, zq^{-1}).$$

Let $\mathcal{O}_{\mathfrak{c}} < \mathbb{A}^*$ denote the subgroup $\mathcal{O}^*$, if $\mathfrak{c} = 1$, and $1 + \mathfrak{c}\mathcal{O}$, otherwise. The integrand of the integral on the left hand side of (4.5.1) is constant on the cosets of the subgroup $\mathcal{U}_{\mathfrak{c}} < F^*\backslash\mathbb{A}^*$, where $\mathcal{U}_{\mathfrak{c}} = (\mathbb{F}_q^* \cap \mathcal{O}_c)\backslash\mathcal{O}_c$. Because $\mathfrak{c}$ is square-free p does not divide $|\mathcal{O}^*/\mathcal{O}_{\mathfrak{c}}|$. Hence $\mu^*(\mathcal{U}_{\mathfrak{c}})$ is a rational number whose denominator is not divisible by p. Therefore $I(\psi_E, \mathfrak{c}, \alpha, \epsilon) \in p^{-m(E)}\mathbb{Z}_p[\epsilon]$ for every $\epsilon \in \mu_\infty$. In particular $v_q(I(\psi_E, \mathfrak{c}, \alpha, \epsilon))$ is at least $-m(E)/d$. Note that for every $\alpha \in \mathbb{X}(\mathfrak{n})$ the L-function $L(\sigma_E \otimes \alpha, t) \in 1 + t\overline{\mathbb{Q}}_p[t]$ hence by Lemma 4.2 there is an $\epsilon \in \mu_\infty$ such that $v_q(L(\sigma_E \otimes \alpha, \epsilon q^{-1})) = -l_q(L(\sigma_E \otimes \alpha, t))$. Hence the first part of the claim above is true.

Assume now that p does not divide the order of $\mathrm{Pic}_0(\mathcal{C})(\mathbb{F}_q)$ and let $h(E)$ denote the right hand side of the inequality in the claim above. As we already noted in the proof of Proposition 2.4 in order to show the second half of the claim we only need to show that $p^{h(E)}\psi_E(g) \in \mathbb{Z}$ for every element $g = \left(\begin{smallmatrix} y & yx \\ 0 & 1 \end{smallmatrix}\right) \in P(\mathbb{A})$. By Lemma 4.4 there are $\eta \in F$, $u \in \mathcal{O}$ and $c \in \mathbb{A}^*$ such that (c) is a square-free effective divisor which is relatively prime to $\mathfrak{n}$ and $x + u + y^{-1}\eta = \widehat{c}$. Because

$$\begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} y & yx \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} y & y(x + u + y^{-1}\eta) \\ 0 & 1 \end{pmatrix}$$

and ψ_E is invariant on the left with respect to $P(F)$ and on the right with respect to $P(\mathcal{O})$, we may assume that $x = \widehat{c}$.

Let $\mathfrak{c}$ be (c) and let H denote the quotient group $\mathbb{A}^*/F^*\mathcal{O}_{\mathfrak{c}}$ where we continue to use the notation above. Then H can be decomposed as a direct product $G \times \mathbb{Z}$ where G is a finite subgroup. By class field theory $|G| = |\mathrm{Pic}_0(\mathcal{C})| \cdot |\mathcal{O}^*/(\mathcal{O}_{\mathfrak{c}}\mathbb{F}_q^*)|$. As we already noted above $p \not| |\mathcal{O}^*/\mathcal{O}_{\mathfrak{c}}|$ hence p does not divide the order of G by our assumption. Let $(\cdot)_H : \mathbb{A}^* \to H$ be the quotient map and let $[\cdot] : H \to G$ denote the projection onto the factor G. Note that for every $y \in \mathbb{A}^*$ the value

$$\psi_E(\begin{pmatrix} y & y\widehat{c} \\ 0 & 1 \end{pmatrix})t^{\deg(y)} \in \mathbb{Q}[G][t, t^{-1}]$$

only depends on $(y)_H$. Let $f : H \to \mathbb{Q}[t, t^{-1}]$ be the corresponding function and define $I = \sum_{\substack{g \in G \\ n \in \mathbb{Z}}} c_{g,n} g t^n \in \mathbb{Q}[G][t, t^{-1}]$ by the formula:

$$I = \sum_{g \in G} \big(\sum_{\substack{h \in H \\ [h] = g}} f(h) \big) g.$$

The function I is well-defined because for every $g \in G$ the set of those $h \in H$ such that $[h] = g$ and $f(y) \neq 0$ is finite. Moreover the set $\{c_{g,n} | g \in G, n \in \mathbb{Z}\}$ and the image of the function $\mathbb{A}^* \to \mathbb{Q}$ given by the rule $y \mapsto \psi_E(\left(\begin{smallmatrix} y & y\widehat{c} \\ 0 & 1 \end{smallmatrix}\right))$ are equal hence it will be sufficient to show that $p^{h(E)}I \in \mathbb{Z}[G][t, t^{-1}]$. For every group homomorphism $\alpha : G \to \overline{\mathbb{Q}}_p^*$ by slight abuse of notation let the same symbol α

denote the unique ring homomorphism $\mathbb{Q}[G][t,t^{-1}] \to \overline{\mathbb{Q}}_p[t,t^{-1}]$ whose restriction onto G is α and $\alpha(t)=t$. Because p does not divide $|G|$ it will be sufficient to show that $v_q(a) \leq -h(E)/d$ for every coefficient a of $\alpha(I)$ for every α as above. Let the symbol α denote also the composition $\alpha \circ [\cdot] \circ (\cdot)_H : \mathbb{A}^* \to \overline{\mathbb{Q}}_p^*$. Choose the character τ so that $\mathfrak{d}$ is relatively prime to $\mathfrak{c}$. Then $\alpha(I)$ is the polynomial:

$$\alpha(I) = \alpha(\mathfrak{d}^2\mathfrak{c}')\epsilon(\alpha^{-1}) \prod_{x \in \underline{\mathfrak{c}}} (q^{\deg(x)}-1)^{-1} \left(\frac{t^2}{q}\right)^{g-1} G(E,\alpha,\mathfrak{c},t)L(\sigma_E \otimes \alpha, tq^{-1})$$

by Proposition 3.9. Because for every polynomial $P(t) = \sum_{k=0}^{N} b_k t^k \in \overline{\mathbb{Q}}_p$we have:

$$\min_{\epsilon \in \mu_\infty}(v_q(P(\epsilon))) = \min_{0 \leq k \leq N}(v_q(b_k)),$$

the claim now follows from Lemmas 4.2 and 4.3. $\square$

5. Galois module structure of the coherent cohomology of elliptic surfaces

Definition 5.1. In this chapter G will be a finite group. Let A be a Noetherian ring and let Y be a scheme which is separated and of finite type over $\mathrm{Spec}(A)$. By an $A[G]$-module on Y we mean a sheaf of $A[G]$-modules on Y. These form the objects of a category whose morphisms are maps respecting the $A[G]$-module structure. Suppose now that $\mathcal{F}$ is an $A[G]$-module on Y which is also an $\mathcal{O}_Y$-module in such a way that the actions of $\mathcal{O}_Y$ and G commute and the $A[G]$-module structure of $\mathcal{F}$ respects the structure morphism $Y \to \mathrm{Spec}(A)$. If $\mathcal{F}$ is also a quasi-coherent (resp. coherent) $\mathcal{O}_Y$-module, then we will call $\mathcal{F}$ a quasi-coherent (resp. coherent) $\mathcal{O}_Y[G]$-module. As noted in [1] on page 447 there are enough injectives in the category of $A[G]$-modules on Y hence the global section functor Γ has a derived functor into the localisation of the category of complexes of $A[G]$-complexes bounded from below with respect to the multiplicative system of quasi-isomorphisms which will be denoted by $R\Gamma^+$.

Definition 5.2. An $A[G]$-module M is cohomologically trivial if the Tate cohomology group $\widehat{H}^i(H,M)$ vanishes for all subgroups H of G and for all integers i. Let $CT(A[G])$ denote the Grothendieck group of all finitely generated $A[G]$-modules which are cohomologically trivial. For every cohomologically trivial $A[G]$-module M let $[M]$ denote its class in $CT(A[G])$). Suppose that $\mathcal{F}$ is a quasi-coherent $\mathcal{O}_Y$-module such that each stalk of $\mathcal{F}$ is a cohomologically trivial $A[G]$-module. Then by Theorem 1.1 of [1] on page 447 the complex $R\Gamma^+(\mathcal{F})$ is isomorphic in the derived category of $A[G]$-modules to a bounded complex M^* of finitely generated cohomologically trivial $A[G]$-modules. Moreover the Euler characteristic $\sum(-1)^i[M^i]$ in $CT(A[G])$ only depends on $\mathcal{F}$ and will be denoted by $\chi(\mathcal{F})$.

Definition 5.3. Let X be a normal scheme which is of finite type over $\mathrm{Spec}(A)$. Assume that the finite group G acts on X on the left. Let $\mathcal{F}$ be a coherent sheaf on X. A G-linearisation on $\mathcal{F}$ is a collection $\Psi = \{\psi_g\}_{g \in G}$ of isomorphisms $\psi_g : g_*(\mathcal{F}) \to \mathcal{F}$ for every $g \in G$ such that

(*i*) we have $\psi_1 = \mathrm{Id}_{\mathcal{F}}$,

(*ii*) for every g, $h \in G$ we have $\psi_{hg} = \psi_h \circ h_*(\psi_g)$,

where $h_*(\psi_g) : (hg)_*(\mathcal{F}) = h_*(g_*(\mathcal{F})) \to h_*(\mathcal{F})$ is the direct image of the map $\psi_g : g_*(\mathcal{F}) \to \mathcal{F}$ under the action of h. We define a G-sheaf over X to be a sheaf on X equipped with a G-linearisation. A coherent G-sheaf is a coherent sheaf on X equipped with a G-linearisation Ψ such that $\psi_g : g_*(\mathcal{F}) \to \mathcal{F}$ is $\mathcal{O}_X$-linear for every $g \in G$.

Definition 5.4. Let $f : X \to Y$ be a tame G-cover as defined in Definition 2.2 of [1] on page 451 and let $\mathcal{F}$ be a coherent G-sheaf on X. The G-linearisation on $\mathcal{F}$ induces an $\mathcal{O}_Y$-linear action of G on the direct image sheaf $f_*(\mathcal{F})$ which makes the latter a coherent $\mathcal{O}_Y[G]$-module. By Theorem 2.7 of [1] on page 452 each stalk of the $\mathcal{O}_Y[G]$-sheaf $f_*(\mathcal{F})$ is a cohomologically trivial $A[G]$-module. Hence the Euler characteristic $\chi(f_*(\mathcal{F})) \in CT(A[G])$ introduced in Definition 5.2 is well-defined. The later will be denoted by $\chi(G, \mathcal{F})$.

Suppose now that A is a field and its characteristic does not divide the order of G. Then every finitely generated $A[G]$-module is cohomologically trivial. Also assume that Y is proper over $\mathrm{Spec}(A)$ and let $\mathcal{F}$ be again a coherent G-sheaf on X. By the above for every $n \in \mathbb{N}$ the cohomology group $H^n(X, \mathcal{F})$ is a cohomologically trivial, finitely generated $A[G]$-module with respect to the natural $A[G]$-action.

Lemma 5.5. *With these assumptions we have*

$$\chi(G, \mathcal{F}) = \sum_{n \in \mathbb{N}} (-1)^n [H^n(X, \mathcal{F})] \in CT(A[G]).$$

Proof. Because finite maps are affine the higher derived sheaves $R^i f_*(\mathcal{F})$ are vanishing. Hence $H^n(X, \mathcal{F}) = H^n(Y, f_*(\mathcal{F}))$ as $A[G]$-modules. Now the claim follows from Proposition 1.5 of [1] on page 449. □

In addition to the assumptions above also suppose now that $f : X \to Y$ above is a map of smooth, projective curves over $\mathrm{Spec}(A)$. Let $\mathcal{L}$ be a line bundle on Y. The line bundle $f^*(\mathcal{L})$ on X is naturally equipped with the structure of a coherent G-sheaf.

Lemma 5.6. *With the same notation and assumptions as above the following equation holds in $CT(A[G])$:*

$$\chi(G, f^*(\mathcal{L})) = \chi(G, \mathcal{O}_X) + \deg(\mathcal{L})[A[G]].$$

Proof. Of course we are going to show the claim with the usual devisage argument. By the Riemann-Roch theorem there is a divisor D on Y whose support is disjoint from the ramification divisor of the cover f and $\mathcal{L} = O_Y(D)$. First assume that D is effective. When $\deg(D) = 0$ the claim is obvious. Otherwise $D = D' + \mathfrak{p}$ where D' is an effective divisor with $\deg(D') < \deg(D)$ and $\mathfrak{p}$ is a closed point on Y. There is a short exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & f^*(\mathcal{O}_Y(D')) \arrow[r] & f^*(\mathcal{O}_Y(D)) \arrow[r] & f^*(A\mathfrak{p}) \arrow[r] & 0 \end{tikzcd}$$

where $A\mathfrak{p}$ denotes the skyskaper sheaf on Y with support $\mathfrak{p}$. Because $\mathfrak{p}$ is not in the ramification locus of f we have $H^0(f_*f^*(A\mathfrak{p}), Y) \cong A[G]^{\deg(\mathfrak{p})}$ as $A[G]$-modules. Moreover all higher cohomology groups of the skyskaper sheaf $f_*f^*(A\mathfrak{p})$ vanish. Hence by the additivity of the Euler characteristic we get:

$$\chi(G, f^*(\mathcal{O}_Y(D))) = \chi(G, f^*(\mathcal{O}_Y(D'))) + \deg(\mathfrak{p})[A[G]].$$

Now the claim follows by induction on $\deg(D)$. Consider next the general case and write $D = D_1 - D_2$ where D_1 and D_2 are divisors on X whose supports are disjoint. We are going to prove the claim by induction on $\deg(D_2)$. We already proved the claim when $\deg(D_2) = 0$. Otherwise $D_2 = D'_2 + \mathfrak{p}$ where D'_2 is an effective divisor with $\deg(D'_2) < \deg(D_2)$ and $\mathfrak{p}$ is a closed point on Y. By repeating the same argument which we used above we get:

$$\chi(G, f^*(\mathcal{O}_Y(D))) = \chi(G, f^*(\mathcal{O}_Y(D_1 - D'_2))) - \deg(\mathfrak{p})[A[G]].$$

The claim is now clear. □

Definition 5.7. Assume now that $A = \mathbf{k}$ is a perfect field of characteristic p and let W denote the ring of Witt vectors of $\mathbf{k}$ of infinite length. Moreover let K denote the field of fractions of W. Let M be a finitely generated cohomologically trivial $\mathbf{k}[G]$-module. Then M is a projective $\mathbf{k}[G]$-module by claim (a) of Proposition 4.1 of [1] on page 557. Hence M is isomorphic to P/pP for some finitely generated projective W-module P. The character of the $\overline{K}[G]$-module $\overline{K} \otimes_W P$ can be written in the form $\sum m_\alpha \alpha$ where the sum is over the set $R(G)$ of irreducible $\overline{K}$-valued characters of G. The integer m_α is independent of the choice of P. Let $\Delta(M) : R(G) \to \mathbb{Z}$ be the function defined by the formula $\Delta(M)(\alpha) = m_\alpha$. This map extends uniquely to a homomorphism from $CT(A[G])$ to the group of $\mathbb{Z}$-valued functions on $R(G)$ which will be denoted by Δ as well.

Suppose that A is a finite extension of the field B. Then the restriction of operators from $A[G]$ to $B[G]$ induces a homomorphism $\mathrm{Res}_{A\to B} : CT(A[G]) \to CT(B[G]))$. Assume now that A is the finite field $\mathbb{F}_q$. Then every $\alpha \in R(G)$ can be considered as a representation of the absolute Galois group of the function field of X. In particular the ϵ-constant $\epsilon(\alpha) \in \overline{\mathbb{Q}}_p$ is defined.

Theorem 5.8. *With the same notation and assumptions as above we have:*

$$\Delta(\mathrm{Res}_{\mathbb{F}_q\to\mathbb{F}_p}(\chi(G, \mathcal{O}_X)))(\alpha) = -dv_q(\epsilon(\alpha^{-1})) \quad (\forall \alpha \in R(G)).$$

Proof. This is a special case of Theorem 5.2 of [1] on pages 463-464. □

Notation 5.9. Suppose now that $Y = \mathcal{C}$ and let $\mathcal{E}$ and Δ_E be the same as in the introduction. Assume that the ramification divisor of the cover $f : X \to Y$ has support disjoint from the conductor of E. Let $g' : \mathcal{E}' \to X$ be the base change of the elliptic fibration $g : \mathcal{E} \to Y$ with respect to the map f. Note that the X-scheme $\mathcal{E}'$ is a relatively minimal regular model of the base change of E to the function field of X. Moreover $\mathcal{E}'$ is equipped with a unique action of G fixing the zero section such that g' is equivariant with respect to this action and the one on X.

Theorem 5.10. *The $\mathbb{F}_q[G]$-module $H^2(\mathcal{E}', \mathcal{O}_{\mathcal{E}'})$ is cohomologically trivial and*

$$\Delta(\mathrm{Res}_{\mathbb{F}_q\to\mathbb{F}_p}([H^2(\mathcal{E}', \mathcal{O}_{\mathcal{E}'})])(\alpha) = \frac{d}{12}\deg(\Delta_E) + dv_q(\epsilon(\alpha^{-1})) \quad (\forall \alpha \in R(G)).$$

Proof. By Lemma 5.5 we have:

$$(5.10.1) \qquad \chi(G, \mathcal{O}_{\mathcal{E}'}) = [H^0(\mathcal{E}', \mathcal{O}_{\mathcal{E}'})] - [H^1(\mathcal{E}', \mathcal{O}_{\mathcal{E}'})] + [H^2(\mathcal{E}', \mathcal{O}_{\mathcal{E}'})].$$

By Lemma 4 of [6] on page 79 the map $(g')^* : \mathrm{Pic}^0(X) \to \mathrm{Pic}^0(\mathcal{E}')$ induced by Picard functoriality is an isomorphism. Because this map is equivariant with respect to the induced G-actions on $\mathrm{Pic}^0(X)$ and $\mathrm{Pic}^0(\mathcal{E}')$, we get that $H^1(\mathcal{E}', \mathcal{O}_{\mathcal{E}'}) = H^1(X, \mathcal{O}_X)$ as $\mathbb{F}_q[G]$-modules, since these modules are isomorphic to the tangent spaces at the zero of the abelian varieties $\mathrm{Pic}^0(\mathcal{E}')$ and $\mathrm{Pic}^0(X)$, respectively. Obviously

$H^0(\mathcal{E}',\mathcal{O}_{\mathcal{E}'})=H^0(X,\mathcal{O}_X)$ as $\mathbb{F}_q[G]$-modules, hence from (5.10.1) and Lemma 5.5 we get that

$$[H^2(\mathcal{E}',\mathcal{O}_{\mathcal{E}'})]=\chi(G,\mathcal{O}_{\mathcal{E}'})-\chi(G,\mathcal{O}_X). \tag{5.10.2}$$

Let $\Omega^1_{\mathcal{E}/Y}$, $\Omega^1_{\mathcal{E}'/X}$ denote the sheaf of relative Kähler differentials of the Y-scheme $\mathcal{E}$ and the X-scheme $\mathcal{E}'$, respectively. Let $\omega_{\mathcal{E}/Y}$, $\omega_{\mathcal{E}'/X}$ denote respectively the pull-back of $\Omega^1_{\mathcal{E}/Y}$ and $\Omega^1_{\mathcal{E}'/X}$ with respect to the zero section. These sheaves are line bundles on Y and X, respectively. Moreover by Grothendieck's duality we have $R^1g'_*(\mathcal{O}_{\mathcal{E}'})=\omega^{\otimes -1}_{\mathcal{E}'/X}$. In particular $\chi(G,R^1g'_*(\mathcal{O}_{\mathcal{E}'}))=-\chi(G,\omega_{\mathcal{E}'/X})$. Because all boundary maps in the spectral sequence $H^p(Y,R^qg'_*(\mathcal{O}_{\mathcal{E}'}))\Rightarrow H^{p+q}(\mathcal{E}',\mathcal{O}_{\mathcal{E}'})$ are $\mathbb{F}_q[G]$-linear we get from the above and Lemma 5.5 that

$$\chi(G,\mathcal{O}_{\mathcal{E}'})=\chi(G,\mathcal{O}_X)-\chi(G,R^1g'_*(\mathcal{O}_{\mathcal{E}'}))=\chi(G,\mathcal{O}_X)-\chi(G,\omega^{\otimes -1}_{\mathcal{E}'/X}). \tag{5.10.3}$$

Combining (5.10.2) and (5.10.3) we get that

$$[H^2(\mathcal{E}',\mathcal{O}_{\mathcal{E}'})]=-\chi(G,\omega^{\otimes -1}_{\mathcal{E}'/X}). \tag{5.10.4}$$

By definition Δ_E is the zero divisor of a non-zero section of $\omega^{\otimes 12}_{\mathcal{E}/Y}$. Therefore $\deg(\Delta_E)=12\deg(\omega_{\mathcal{E}/Y})$. Moreover $\omega_{\mathcal{E}'/X}=f^*(\omega_{\mathcal{E}/Y})$. Hence (5.10.4) and Lemma 5.6 implies that

$$[H^2(\mathcal{E},\mathcal{O}_{\mathcal{E}})]=\frac{\deg(\Delta_E)}{12}[\mathbb{F}_q[G]]-\chi(G,\mathcal{O}_X).$$

The claim now follows from Theorem 5.8. □

6. Slope estimates

Definition 6.1. Let $\sigma:W\to W$ denote the absolute Frobenius automorphism. Let $W((V))$ denote the W-algebra of formal Laurent series $\sum_{i\geq n}a_iV^i$, where $a_i\in W$ and $n\in\mathbb{Z}$ are arbitrary, with the usual addition and with multiplication defined by the formula:

$$\big(\sum_{i\geq n}a_iV^i\big)\cdot\big(\sum_{j\geq m}b_jV^j\big)=\sum_{k\geq n+m}\big(\sum_{i+j=k}a_i\sigma^{-i}(b_j)\big)V^k.$$

Moreover let $W[V]$ and $W[[V]]$ denote the subring of $W((V))$ consisting of polynomials and formal power series in the variable V, respectively. Let M be a module over the ring $W[V]$. Then the kernel and the cokernel of the multiplication by $V:M\to M$ are W-modules and we define

$$\chi(M)=\text{length}_W(\text{Ker}(V))-\text{length}_W(\text{Coker}(V))$$

provided both numbers on the right are finite. Let $W[V,F]$ denote ring generated by the variable V over W subject to the relations $VF=FV=p$, $Fc=\sigma(c)F$ and $Vc=\sigma^{-1}(c)V$ for every $c\in W$. For every module M over the Dieudonné ring $W[F,V]$ which is free and finitely generated as a W-module the tensor product $M\otimes_W K$ is an F-isocrystal over W with respect to multiplication by $F\otimes_W\text{id}_K$. For every F-isocrystal M over W let $l(M)$ denote $\sum m_i(1-\lambda_i)$ where the λ_i are the slopes of M and m_i is the multiplicity of λ_i.

Lemma 6.2. *Then the following hold:*

(*i*) *if* $0 \to M' \to M \to M \to 0$ *is a short exact sequence of* $W[V]$*-modules, then* $\chi(M)$ *is defined if* $\chi(M')$ *and* $\chi(M'')$ *are defined and*

$$\chi(M) = \chi(M') + \chi(M''),$$

(*ii*) *if* M *is a module over the ring* $W[F, V]$ *which is free and finitely generated as a* W*-module, then* $\chi(M) = -l(M \otimes_W K)$*,*

(*iii*) *if* M *is a finitely generated torsion* $W[[V]]$*-module then*

$$\chi(M) = -\text{length}_{W((V))} M \otimes_{W[[V]]} W((V)).$$

Proof. This is Lemma 7.2 of [17] on page 530. □

Definition 6.3. Let G be a finite abelian group whose order is not divisible by p and assume that $\mathbf{k}$ is algebraically closed. Then every $\alpha \in R(G)$ takes values in W hence the element $\pi_\alpha = \sum_{g \in G} \alpha(g)^{-1} g \in W[G]$ is well-defined. For every $W[G]$-module M let M^α denote the sub $W[G]$-module $\pi_\alpha M$. Finally for every F-isocrystal M over W and real numbers $a \leq b$ let $M_{[a,b)}$ denote the maximal subquotient of M with slopes in the interval $[a, b)$.

Let X be a smooth projective variety defined over $\mathbf{k}$ and assume that G acts on X. Let $H^m(X/W)$ denote the m-th crystalline cohomology group of W. Then $W[G]$ acts on $H^m(X/W)$ and $H^m(X, \mathcal{O}_X)$ by functoriality for every m.

Proposition 6.4. *We have:*

$$l(H^r(X/W)^\alpha \otimes_W K_{[0,1)}) \leq \dim_{\mathbf{k}}(H^r(X, \mathcal{O}_X)^\alpha)$$

for every $r \in \mathbb{N}$ *and* $\alpha \in R(G)$*.*

Proof. Let $H^r(X, W)$ denote the r-th Witt vector cohomology group of the variety X. The latter is a $W[V]$-module and there is a long exact sequence:

$$\cdots \to H^{r-1}(X, \mathcal{O}_X) \to H^r(X, W) \xrightarrow{V} H^r(X, W) \to H^r(X, \mathcal{O}_X) \to \cdots$$

The group G acts on all cohomology groups in the sequence above and the maps are equivariant with respect to this action so there is a long exact sequence:

$$\cdots \to H^{r-1}(X, \mathcal{O}_X)^\alpha \to H^r(X, W)^\alpha \xrightarrow{V} H^r(X, W)^\alpha \to H^r(X, \mathcal{O}_X)^\alpha \to \cdots$$

Because X is projective the vector spaces $H^r(X, \mathcal{O}_X)^\alpha$ have finite dimension. Therefore $\chi(H^r(X, W)^\alpha)$ is well-defined and

$$\chi(H^r(X, W)^\alpha) \geq -\dim_{\mathbf{k}}(H^r(X, \mathcal{O}_X)^\alpha). \tag{6.4.1}$$

Write

$$H^r(X, W)^\alpha_t = \text{Ker}(H^r(X, W)^\alpha \to H^r(X, W)^\alpha \otimes_W K).$$

Then $H^r(X, W)^\alpha_t$ is a torsion $W[[V]]$-module and there is a short exact sequence of $W[V]$-modules:

$$0 \to H^r(X, W)^\alpha_t \to H^r(X, W)^\alpha \to H^r(X, W)^\alpha_{ct} \to 0$$

such that $H^r(X, W)^\alpha_{ct}$ is a module over the Dieudonné ring $W[F, V]$ which is free and finitely generated as a W-module. Therefore by part (*i*) of Lemma 6.2 we have:

$$\chi(H^r(X, W)^\alpha) = \chi(H^r(X, W)^\alpha_t) + \chi(H^r(X, W)^\alpha_{ct}). \tag{6.4.2}$$

Because the slope spectral sequence degenerates modulo torsion (Théorème 3.2 of [8] on page 615) there is an isomorphism between the F-isocrystals $H^r(X, W) \otimes_W K$ and $H^r(X/W) \otimes K_{[0,1)}$. Since this isomorphism is equivariant with respect to the action of G we get that the F-isocrystals $H^r(X,W)^\alpha \otimes_W K$ and $H^r(X/W)^\alpha \otimes_W K_{[0,1)}$ are also isomorphic. Hence

$$(6.4.3) \quad \chi(H^r(X,W)^\alpha_{ct}) = -l(H^r(X,W)^\alpha_{ct} \otimes_W K) = -l(H^r(X/W)^\alpha \otimes_W K_{[0,1)}).$$

by part (*ii*) of Lemma 6.2. According to part (*iii*) of Lemma 6.2 the number $\chi(H^r(X,W)^\alpha_t)$ is not positive. Hence (6.4.1), (6.4.2) and (6.4.3) imply that

$$-l(H^r(X/W)^\alpha \otimes_W K_{[0,1)}) \geq -\dim_{\mathbf{k}}(H^r(X,\mathcal{O}_X)^\alpha). \quad \square$$

Notation 6.5. Assume now that $\mathbf{k}$ is the algebraic closure of $\mathbb{F}_q$ and for every $\mathrm{Spec}(\mathbb{F}_q)$-scheme S let $\overline{S}$ denote its base change to $\mathrm{Spec}(\mathbf{k})$. Moreover let $F : \overline{S} \to \overline{S}$ denote the Frobenius relative to $\mathbb{F}_q$ for every such S. Assume now that X is a smooth projective variety defined over $\mathbf{k}$ equipped with an action of G. Recall that we've chosen a prime $l \neq p$. Now fix an isomorphism $\nu : \overline{\mathbb{Q}}_l \to \overline{\mathbb{Q}}_p$. Since group G acts on the étale cohomology group $H^m(\overline{X},\overline{\mathbb{Q}}_l)$ we may consider the latter as a $\mathbb{W}[G]$-module if we identify $\overline{\mathbb{Q}}_l$ and $\overline{\mathbb{Q}}_p$ via ν. Then the map $F^* : H^m(\overline{X},\overline{\mathbb{Q}}_l) \to H^m(\overline{X},\overline{\mathbb{Q}}_l)$ induced by the Frobenius morphism F commutes with the action of G so $H^m(\overline{X},\overline{\mathbb{Q}}_l)^\alpha$ is an F^*-invariant subspace.

Lemma 6.6. *We have:*

$$l_q(\det(1-F^*t|H^m(\overline{X},\overline{\mathbb{Q}}_l)^\alpha)) = l(H^m(\overline{X}/W)^\alpha \otimes_W K_{[0,1)}).$$

Proof. For every $g \in G$ let the same symbol denote the base change $\overline{X} \to \overline{X}$ to Speck($\mathbf{k}$) of the automorphism $X \to X$ furnished by the given action of G on X. For every positive integer n the composition

$$g \circ F^{[n]} = g \circ \underbrace{F \circ \cdots \circ F}_{n\text{-times}}$$

induces the zero map on tangent spaces, hence the Lefschetz trace formula applied to $g \circ F^{[n]}$ both in the l-adic and the crystalline cohomology theories imply together that

$$(6.6.1) \quad \sum_{m=0}^{2\dim(\overline{X})} (-1)^m \mathrm{Tr}(1-g^*(F^*)^n|H^m(\overline{X},\overline{\mathbb{Q}}_l)) =$$

$$\sum_{m=0}^{2\dim(\overline{X})} (-1)^m \mathrm{Tr}(1-g^*(F^*)^n|H^m(\overline{X}/W)\otimes_W K).$$

Let $l_m(\alpha,t)$ and $c_m(\alpha,t)$ denote the polynomials:

$$\det(1-F^*t|H^m(\overline{X},\overline{\mathbb{Q}}_l)^\alpha) \text{ and } \det(1-F^*t|H^m(\overline{X}/W)\otimes_W K^\alpha),$$

respectively. By the orthogonality of characters the equation (6.6.1) implies that

$$(6.6.2) \qquad \prod_{m=0}^{2\dim(\overline{X})} l_m(\alpha,t)^{(-1)^m} = \prod_{m=0}^{2\dim(\overline{X})} c_m(\alpha,t)^{(-1)^m}.$$

By Deligne's purity theorem and Theorem 1 of [11] on page 74 the reciprocal roots of the polynomials $l_m(\alpha,t)$ and $c_m(\alpha,t)$ are Weil numbers with squared complex norm q^m. Hence there are no cancellations in the alternating products in (6.6.2) above. Therefore $l_m(\alpha,t) = c_m(\alpha,t)$ for every m. Let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the eigenvalues of F^* considered as a linear transformation of $H^m(\overline{X}/W)\otimes_W K^\alpha$. The claim now follows from the fact that $v_q(\lambda_1), v_q(\lambda_2), \dots, v_q(\lambda_k)$ are the slopes of the F-isocrystal $H^m(\overline{X}/W) \otimes_W K^\alpha$. □

Notation 6.7. Let us consider now the same situation as in the introduction. Fix a tamely ramified character $\alpha \in \mathbb{X}(\mathfrak{n})$ and let $\pi : X \to \mathcal{C}$ be the Galois cover corresponding to the extension $F'|F$ where F' is the subfield of $\overline{F}$ fixed by the kernel of α. Let G denote the Galois group of the cover π and let $g' : \mathcal{E}' \to X$ denote the base change of $g : \mathcal{E} \to \mathcal{C}$ with respect to the map f as in Notation 5.9. We will also keep on using the notation introduced in 6.5.

Lemma 6.8. *We have:*

$$l_q(L(\sigma_E \otimes \alpha, t)) = l(H^2(\overline{\mathcal{E}}'/W)^\alpha \otimes_W K_{[0,1)}).$$

Proof. For every morphism $m : R \to S$ of $\mathrm{Spec}(\mathbb{F}_q)$-schemes let $\overline{m} : \overline{R} \to \overline{S}$ denote the base change to $\mathrm{Spec}(\mathbf{k})$. The Leray spectral sequence $H^p(\overline{X}, R^q\overline{g}'_*(\overline{\mathbb{Q}}_l(1))) \Rightarrow H^{p+q}(\overline{\mathcal{E}'}, \overline{\mathbb{Q}}_l(1))$ furnishes an injection $\zeta : H^1(\overline{X}, R^1\overline{g}'_*(\overline{\mathbb{Q}}_l(1))) \to H^2(\overline{\mathcal{E}}', \overline{\mathbb{Q}}_l(1))$ and the image of this map is the orthogonal complement of the $\overline{\mathbb{Q}}_l$-linear subspace V spanned by the Chern classes of the zero section and the fibres of the elliptic fibration $\overline{\mathcal{E}}' \to \overline{\mathcal{C}}$, considered here as divisors on the surface $\overline{\mathcal{E}}'$, with respect to the cup product pairing. The cohomology group $H^1(\overline{X}, R^1\overline{g}'_*(\overline{\mathbb{Q}}_l(1)))$ is naturally equipped with a G-action because the map $\overline{g}'$ is equivariant with respect to the action of G on $\overline{\mathcal{E}}'$ and $\overline{X}$, respectively. Moreover ζ is G-linear. Hence we have an isomorphism:

$$H^1(\overline{X}, R^1\overline{g}'_*(\overline{\mathbb{Q}}_l))^\alpha \oplus V^\alpha(-1) \cong H^2(\overline{\mathcal{E}}', \overline{\mathbb{Q}}_l)^\alpha. \tag{6.8.1}$$

Note that the cohomology group $H^1(\overline{X}, R^1\overline{g}'_*(\overline{\mathbb{Q}}_l))$ is equipped with the action of a Frobenius operator F^* which commutes with the action of G and the isomorphism in (6.8.1) respects the action of the operator F^* on both sides. Moreover for every eigenvalue λ of F^* on $V(-1)$ we have $v_q(\lambda) = 1$, hence

$$l_q(\det(1 - F^*t|H^1(\overline{X}, R^1\overline{g}'_*(\overline{\mathbb{Q}}_l))^\alpha)) = l_q(\det(1 - F^*t|H^2(\overline{\mathcal{E}}', \overline{\mathbb{Q}}_l)^\alpha)).$$

We may consider α a lisse l-adic sheaf on $\mathrm{Spec}(F)$. By slight abuse of notation let α also denote the pull-back onto $\overline{\mathcal{C}}$ of the direct image of this sheaf α with respect to the open immersion $\mathrm{Spec}(F) \to \mathcal{C}$. Because the Galois representation $H^1(E_{\overline{F}}, \overline{\mathbb{Q}}_l)$ is absolutely irreducible and self-dual we have

$$H^0(\overline{\mathcal{C}}, R^1\overline{g}_*(\overline{\mathbb{Q}}_l) \otimes \alpha) = H^2(\overline{\mathcal{C}}, R^1\overline{g}_*(\overline{\mathbb{Q}}_l) \otimes \alpha) = 0.$$

Moreover $H^1(\overline{\mathcal{C}}, R^1\overline{g}_*(\overline{\mathbb{Q}}_l) \otimes \alpha) = H^1(\overline{X}, R^1\overline{g}'_*(\overline{\mathbb{Q}}_l))^\alpha$ by the degeneration of the Hochschild-Serre spectral sequence. Hence by the Grothendieck-Verdier trace formula:

$$l_q(L(\sigma_E \otimes \alpha, t)) = l_q(\det(1 - F^*t|H^1(\overline{X}, R^1\overline{g}'_*(\overline{\mathbb{Q}}_l))^\alpha) = l_q(\det(1 - F^*t|H^2(\overline{\mathcal{E}}', \overline{\mathbb{Q}}_l)^\alpha)).$$

The claim now follows from Lemma 6.6. □

Theorem 6.9. *Assume that p does not divide the order of* $\mathrm{Pic}_0(\mathcal{C})(\mathbb{F}_q)$. *Then we have:*

$$m(E) \leq d(\frac{1}{12}\deg(\Delta_E) + g - 1).$$

Proof. Let $\alpha \in \mathbb{X}(\mathfrak{n})$ be arbitrary and let $C(\alpha)$ denote the set of all characters $\beta : \mathrm{Gal}(F'|F) \to \overline{\mathbb{Q}}_p^*$ which are conjugate to α under the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p)$ on $\overline{\mathbb{Q}}_p$. For every $\beta \in C(\alpha)$ we have:

$$(6.9.1) \qquad l_q(L(\sigma_E \otimes \beta, t)) \leq \dim_{\mathbf{k}}(H^2(\overline{\mathcal{E}}', \mathcal{O}_{\overline{\mathcal{E}}'})^\beta) = \dim_{\mathbf{k}}(H^2(\mathcal{E}', \mathcal{O}_{\mathcal{E}'}) \otimes_{\mathbb{F}_q} \mathbf{k}^\beta)$$

by Proposition 6.4 and Lemma 6.8. According to Remark 4.5 of [1] on page 460 we have

$$(6.9.2) \ \Delta(\mathrm{Res}_{\mathbb{F}_q \to \mathbb{F}_p}([H^2(\mathcal{E}', \mathcal{O}_{\mathcal{E}'})])(\alpha) = \frac{d}{|C(\alpha)|} \sum_{\beta \in C(\alpha)} \dim_{\mathbf{k}}(H^2(\mathcal{E}', \mathcal{O}_{\mathcal{E}'}) \otimes_{\mathbb{F}_q} \mathbf{k}^\beta).$$

Because the action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p)$ on $\overline{\mathbb{Q}}_p$ leaves the valuation v_q invariant we have:

$$l_q(L(\sigma_E \otimes \beta, t)) = l_q(L(\sigma_E \otimes \alpha, t))$$

for every $\beta \in C(\alpha)$. Hence (6.9.1), (6.9.2) and Theorem 5.10 imply that

$$\begin{aligned} l_q(L(\sigma_E \otimes \alpha, t)) &= \frac{1}{|C(\alpha)|} \sum_{\beta \in C(\alpha)} l_q(L(\sigma_E \otimes \beta, t)) \\ &\leq \frac{1}{|C(\alpha)|} \sum_{\beta \in C(\alpha)} \dim_{\mathbf{k}}(H^2(\mathcal{E}', \mathcal{O}_{\mathcal{E}'}) \otimes_{\mathbb{F}_q} \mathbf{k}^\beta) \\ &= \frac{1}{d} \cdot \Delta(\mathrm{Res}_{\mathbb{F}_q \to \mathbb{F}_p}([H^2(\mathcal{E}', \mathcal{O}_{\mathcal{E}'})])(\alpha) \\ &= \frac{1}{12} \deg(\Delta_E) + v_q(\epsilon(\alpha^{-1})). \end{aligned}$$

The claim now follows from Proposition 4.5. □

Definition 6.10. Following [14] we will call a smooth projective variety V defined over a perfect field of characteristic p ordinary in dimension n if the n-dimensional Newton and the n-dimensional Hodge polygons of V agree.

Theorem 6.11. *Assume that the elliptic surface $\mathcal{E}$ is ordinary in dimension 2. Then we have:*

$$m(E) \geq d(\frac{1}{12} \deg(\Delta_E) + g - 1).$$

Proof. By Deligne's purity theorem we have $\epsilon(1) = \pm q^{g-1}$ where 1 denotes the trivial representation. Hence in the special case when G is the trivial group, that is, the cover f is the identity map of $\mathcal{C}$ onto itself, Theorem says 5.10 that

$$\dim_{\mathbb{F}_q} H^2(\mathcal{E}, \mathcal{O}_{\mathcal{E}}) = \frac{1}{12} \deg(\Delta_E) + g - 1.$$

Because $\mathcal{E}$ is ordinary in dimension 2 we have

$$l_q(L(E, t)) = l_q(\det(1 - F^* t | H^2(\overline{\mathcal{E}}, \mathbb{Q}_l))) = \dim_{\mathbb{F}_q} H^2(\mathcal{E}, \mathcal{O}_{\mathcal{E}})$$

by definition. The claim now follows from Proposition 4.5. □

Remark 6.12. It is known that a smooth projective variety V is ordinary if V is a generic curve of genus g (see [4], [16]), a generic abelian variety of dimension d equipped with a polarisation of degree r (see [18], [19]), or a generic complete intersection of multidegree $(a_1, a_2, \ldots, a_n)$ (see [9]). It is natural to expect that the same holds for elliptic surfaces with a section. More precisely one might conjecture the following. Assume that $p > 3$, let $N \geq 2$ be a positive integer, let $g \in \mathbb{N}$ and let

$\mathcal{M}_{g,N,p}$ denote the course moduli representing the functor which associates to every scheme T over $\mathrm{Spec}(\mathbb{F}_p)$ the set of isomorphism classes of smooth families of elliptic surfaces over a smooth curve of genus g over T with discriminant of degree $12N$ in all geometric fibres over T, constructed in the paper [24]. Then I expect that for every p, g and N as above there is a non-empty open subscheme $\mathcal{U}$ of $\mathcal{M}_{g,N,p}$ such that for every geometric point of $\mathcal{U}$ the corresponding elliptic surface is ordinary. Of course it is enough to show that there a geometric point of $\mathcal{M}_{g,N,p}$ such that the corresponding elliptic surface is ordinary in dimension two.

7. An upper bound in terms of the conductor

Notation 7.1. For every elliptic curve E defined over a field K of characteristic p let $E^{(p)}$ denote pull-back of E with respect to the Frobenius map $K \to K$ (given by $x \mapsto x^p$). We will call $E^{(p)}$ the Frobenius twist of E. The elliptic curve $E^{(p)}$ is in fact defined over the subfield K^p of p-th powers. The absolute Frobenius $\mathbf{F} : E \to E^{(p)}$ is an isogeny defined over the field K. Finally for every cohomology class $c \in H^1(K, \mathrm{Aut}(E))$ let E_c denote twist of E by c.

Definition 7.2. Let K be as above and let E be an elliptic curve defined over K such that $j(E) \neq 0, 1728$. Because $j(E^{(p)}) = j(E)^p$ we have $j(E^{(p)}) \neq 0, 1728$. Hence by part (c) of Proposition 1.2 of [26] on pages 325-326 the groups $\mathrm{Aut}(E)$ and $\mathrm{Aut}(E^{(p)})$ are both equal to multiplication by ± 1. Therefore there is a unique isomorphism $f : \mathrm{Aut}(E) \to \mathrm{Aut}(E^{(p)})$ such that $\mathbf{F} \circ \phi = f(\phi) \circ \mathbf{F}$ for every $\phi \in \mathrm{Aut}(E)$. Let $f_* : H^1(K, \mathrm{Aut}(E)) \to H^1(K, \mathrm{Aut}(E^{(p)}))$ denote the isomorphism induced by the identification f.

The following two claims will be useful, and they seem not to be recorded in the literature.

Lemma 7.3. *Assume that $j(E) \neq 0, 1728$. Then the elliptic curves $(E_c)^{(p)}$ and $(E^{(p)})_{f_*(c)}$ are isomorphic over K for every $c \in H^1(K, \mathrm{Aut}(E))$.*

Proof. For every scheme X over $\mathrm{Spec}(K)$ let $\overline{X}$ denote $X \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\overline{K})$. For every $\gamma \in \mathrm{Gal}(\overline{K}|K)$ and X as above let the symbol γ also denote the unique endomorphism of $\overline{X}$ which makes the diagram:

$$\begin{tikzcd}
\overline{X} \arrow[r, "\gamma"] \arrow[d] & \overline{X} \arrow[d] \\
\mathrm{Spec}(\overline{K}) \arrow[r, "\gamma"] & \mathrm{Spec}(\overline{K})
\end{tikzcd}$$

commutative. Fix an isomorphism $\phi : \overline{E} \to \overline{E_c}$ over $\overline{K}$. Then for every $\gamma \in \mathrm{Gal}(\overline{K}|K)$ the pull-back of the diagram:

$$\overline{E} \xrightarrow{\phi} \overline{E_c} \xrightarrow{\gamma} \overline{E_c} \xrightarrow{\phi^{-1}} \overline{E} \xrightarrow{\gamma^{-1}} \overline{E}$$

with respect to the Frobenius map $x \mapsto x^p$ of $\mathrm{Spec}(\overline{K})$ is:

$$\overline{E^{(p)}} \xrightarrow{\psi} \overline{(E_c)^{(p)}} \xrightarrow{\gamma} \overline{(E_c)^{(p)}} \xrightarrow{\psi^{-1}} \overline{E^{(p)}} \xrightarrow{\gamma^{-1}} \overline{E^{(p)}},$$

where $\psi : \overline{E^{(p)}} \to \overline{(E_c)^{(p)}}$ is the unique isomorphism such that $\mathbf{F} \circ \phi = \psi \circ \mathbf{F}$. The $\mathrm{Aut}(E)$-valued function $\gamma \mapsto \gamma^{-1} \circ \phi^{-1} \circ \gamma \circ \phi$ on $\mathrm{Gal}(\overline{F}|F)$ is a cocycle which represents c. Note that

$$\mathbf{F} \circ \gamma^{-1} \circ \phi^{-1} \circ \gamma \circ \phi = \gamma^{-1} \circ \psi^{-1} \circ \gamma \circ \psi \circ \mathbf{F} \quad (\forall \gamma \in \mathrm{Gal}(\overline{F}|F)),$$

therefore the function $\gamma \mapsto \gamma^{-1} \circ \psi^{-1} \circ \gamma \circ \psi$ is a cocycle which represents $f_*(c)$. The claim is now clear. □

Proposition 7.4. *Let K be a field of characteristic p and let E be an elliptic curve defined over K. Assume that $j(E) \neq 0, 1728$ and $j(E) \in K^p$. Then E is isomorphic to the Frobenius twist of an elliptic curve E' defined over K.*

Proof. Let $\lambda \in K$ be the unique p-th root of $j(E)$. By Proposition 1.1 of [26] on pages 324-325 there is an elliptic curve $\widetilde{E}$ defined over K such that $j(\widetilde{E}) = \lambda$. Then the Frobenius twist $\widetilde{E}^{(p)}$ of $\widetilde{E}$ is defined over K and has the same j-invariant as E. Hence by the theory of twists there is a cohomology class $c \in H^1(K, \mathrm{Aut}(\widetilde{E}^{(p)}))$ such that E is the twist of $\widetilde{E}^{(p)}$ by c. Let E' be the twist of $\widetilde{E}$ by $f_*^{-1}(c)$. By Lemma 7.3 above E is isomorphic to the Frobenius twist of E'. □

Now let K denote the function field of a smooth, projective, geometrically irreducible curve X defined over a perfect field of characteristic p.

Corollary 7.5. *Let E be a non-isotrivial elliptic curve defined over K. Then E is isogeneous to an elliptic curve E' defined over K with the property $j(E') \notin K^p$.*

Proof. By assumption $j(E)$ does not lie in the constant field of K hence there is a $\lambda \in K$ and natural number n such that $\lambda \notin K^p$ and $\lambda^{p^n} = j(E)$. By Proposition 7.4 there is an elliptic curve E' defined over K such that $j(E') = \lambda$ and E is the n-fold Frobenius twist of E'. In particular E and E' are isogeneous. □

For every elliptic curve E defined over K let Δ_E denote the discriminant of a relatively minimal elliptic surface $\mathcal{E} \to X$ whose generic fibre is E. Then Δ_E is an effective divisor on the curve X. We will say that a non-isotrivial elliptic curve E is minimal in its isogeny class if we have $\deg(\Delta_E) = \min(\deg(\Delta_{E'}))$ where E' is any elliptic curve defined over K isogeneous to E. Let $\mathfrak{n}$ denote the conductor of E.

Theorem 7.6. (Pesenti-Szpiro) *Assume that E is an non-isotrivial elliptic curve which is minimal in its isogeny class. With previous notation we have:*

$$\deg(\Delta_E) \leq 6(\deg(\mathfrak{n}) + 2g - 2).$$

Proof. By Corollary 7.5 the claim follows at once from Théorème 0.1 of [22] on page 84 and the isogeny-invariance of the conductor. □

Let us return to the situation of the introduction. Because in each isogeny class of non-isotrivial elliptic curves there is an elliptic curve which is minimal the theorem above combined with Theorem 1.3 has the following immediate

Corollary 7.7. *Assume that p does not divide the order of $\mathrm{Pic}_0(\mathcal{C})(\mathbb{F}_q)$. Then we have:*

$$m(E) \leq d(\frac{1}{2}\deg(\mathfrak{n}) + 2g - 2).$$

Remark 7.8. Note that this inequality is significantly weaker than Theorem 1.3 because the Pesenti-Szpiro inequality fails to be an equality in general. For example in the special case of the elliptic curve E of Theorem 1.4 a fast inspection of Ulmer's paper [29] (see 2.2-2.3 on page 298) reveals that its conductor $\mathfrak{n}$ is the sum of the prime divisors of the polynomial $T(1 - 2^4 3^3 T^n)$. Because by the assumptions of

Theorem 1.4 the prime p does not divide 2^43^3n, the greatest common divisor of $1-2^43^3T^n$ and its derivative is:

$$(1-2^43^3T^n, -n2^43^3T^{n-1})=(1),$$

so we get that the polynomial $1-2^43^3T^n$ is square-fee and therefore $\deg(\mathfrak{n})=n+1$. Hence in this case Corollary 7.7 says that

$$m(E)\leq\frac{n}{2}-\frac{3}{2}.$$

On the other hand we will see in the next chapter that in this case Theorem 1.3 says that

$$m(E)\leq\frac{n}{6}-1$$

and the two sides above are actually equal by Theorem 1.4.

Remark 7.9. Corollary 7.7 was already proved by K.-S. Tan in the special case when $\mathcal{C}=\mathbb{P}^1_{\mathbb{F}_q}$ and $\mathfrak{n}$ is square-free in [28]. His strategy is similar to ours in reducing the result to estimates of the p-adic valuations of coefficients of twisted L-functions. For the latter he uses the Grothendieck-Ogg-Shafarevich formula and the functional equation. His methods also use facts about the structure of the set $GL_2(F)\backslash GL_2(\mathbb{A})$ specific to the rational function field, hence it is impossible to generalise his approach in order to show Corollary 7.7 in general.

8. Elliptic curves with positive Manin constant

Definition 8.1. Fix a positive integer n which is not divisible by p. Let E_n be the elliptic curve over $F=\mathbb{F}_q(T)$ (where $q=p^d$) with plane cubic model

$$y^2+xy=x^3-T^n.$$

Straightforward calculation shows that $j(E)^{-1}=T^n(1-2^43^3T^n)$. Hence E is not isotrivial. Let Δ_{E_n} denote the discriminant of a relatively minimal elliptic surface $\mathcal{E}_n\to\mathcal{C}$ whose generic fibre is E_n. The degree of Δ_{E_n} can be easily computed from the results of 2.2-2.3 of [29] on page 298. In particular when $p\geq5$ it follows at once from these results and Table 4.1 of [27] on page 365 that $\deg(\Delta_{E_n})=12\lceil n/6\rceil$.

Definition 8.2. Let F_n be the Fermat surface of degree n over $\mathbb{F}_q$, i.e., the hypersurface in $\mathbb{P}^3_{\mathbb{F}_q}$ defined by the equation:

$$x_0^n+x_1^n+x_2^n+x_3^n=0.$$

Let μ_n denote the group of n-th roots of unity in $\overline{\mathbb{F}}_p$. Let G be the quotient of μ_n^4 modulo the diagonally embedded copy of μ_n. For every $\underline{z}=(\zeta_0,\zeta_1,\zeta_2,\zeta_3)\in\mu_n^4$ let $[\zeta_0,\zeta_1,\zeta_2,\zeta_3]$ denote the image of $\underline{z}$ under the quotient map $\mu_n^4\to G$. Then the group scheme G acts on F_n and the action on the level of points is given by the rule:

$$[\zeta_0,\zeta_1,\zeta_2,\zeta_3]\cdot[x_0:x_1:x_2:x_3]=[\zeta_0x_0:\zeta_1x_1:\zeta_2x_2:\zeta_3x_3].$$

Fix a primitive n-th root of unity $\zeta\in\overline{\mathbb{F}}_p$ and let $\Gamma\subset G$ be the subgroup generated by $[\zeta^2,\zeta,1,1]$ and $[1,\zeta,\zeta^3,1]$. As a sub group-scheme Γ is defined over $\mathbb{F}_q$ hence the quotient surface F_n/Γ is defined over $\mathbb{F}_q$, too.

Theorem 8.3. *The surfaces $\mathcal{E}_n$ and F_n/Γ are birationally equivalent.*

Proof. This claim is made in 4.3 of [29] on page 301. The proof can be found in sections 3 and 4 of [29] on pages 298–301. □

Notation 8.4. Let $\mathbb{O}_p$ denote the ring of integers of $\overline{\mathbb{Q}}_p$ and let $\mathfrak{p}$ be its maximal ideal. We view all finite fields of characteristic p as subfields of $\mathbb{O}_p/\mathfrak{p}$, which is an algebraic closure of $\mathbb{F}_p$. Reduction modulo $\mathfrak{p}$ induces an isomorphism between the group of all roots of unity of order prime to p in $\mathbb{O}_p$ and the multiplicative group of $\mathbb{O}_p/\mathfrak{p}$. We let $\alpha : (\mathbb{O}_p/\mathfrak{p})^* \to \overline{\mathbb{Q}}_p^*$ denote the inverse of this isomorphism. We will use the same letter α for the restriction to any finite field $\mathbb{F}_q^*$.

Definition 8.5. Fix a nontrivial character $\psi_0 : \mathbb{F}_p \to \overline{\mathbb{Q}}_p^*$ and for each finite extension $\mathbb{F}_{p^m}$ of $\mathbb{F}_p$, let $\psi : \mathbb{F}_{p^m} \to \overline{\mathbb{Q}}_p^*$ be defined by $\psi = \psi_0 \circ \mathrm{Tr}_{\mathbb{F}_{p^m}|\mathbb{F}_p}$. If $\chi : \mathbb{F}_{p^m}^* \to \overline{\mathbb{Q}}_p^*$ is a nontrivial character, we define the corresponding Gauss sum by

$$g(\chi, \psi) = -\sum_{x \in \mathbb{F}_{p^m}^*} \chi(x)\psi(x).$$

If $\chi_1, \ldots, \chi_r$ are characters $\mathbb{F}_{p^m}^* \to \overline{\mathbb{Q}}_p^*$, not all trivial, such that the product $\chi_1 \cdots \chi_r$ is trivial, we define the Jacobi sum $J(\chi_1, \ldots, \chi_r)$ by

$$J(\chi_1, \ldots, \chi_r) = \begin{array}{ll} \frac{(-1)^r}{p^m} \prod_{i=1}^r g(\chi_i, \psi), & \text{if all } \chi_i \text{ are nontrivial,} \\ 0, & \text{otherwise.} \end{array}$$

Theorem 8.6. (Stickelberger) *For any* $1 \leq k \leq p^m - 2$ *we have:*

$$v_p(g(\alpha^{-k}, \psi)) = s(k)/(p-1),$$

where if $k = k_0 + pk_1 + \cdots + p^{m-1}k_{m-1}$ *is the* p*-adic expansion of the integer* k*, we define* $s(k) = k_0 + k_1 + \cdots + k_{m-1}$.

Proof. This is the second claim of Theorem 9 of [12] on pages 94–95. □

Definition 8.7. Let G be the group which we introduced in Definition 8.2. Let $\widehat{G}$ denote the group of characters G with values in $\overline{\mathbb{Q}}_p$. Using the character $\alpha : (\mathbb{O}_p/\mathfrak{p})^* \to \overline{\mathbb{Q}}_p^*$ we can identify $\widehat{G}$ with

$$\left\{ a = (a_0, a_1, a_2, a_3) \in (\mathbb{Z}/n\mathbb{Z})^4 \,\middle|\, \sum a_i = 0 \right\}$$

where the duality pairing $G \times \widehat{G} \to \overline{\mathbb{Q}}_p^*$ is

$$a(z) = \langle (a_0, a_1, a_2, a_3), [\zeta_0, \zeta_1, \zeta_2, \zeta_3] \rangle = \prod_{i=0}^{3} \alpha(\zeta_i)^{a_i}.$$

For every $a \in \widehat{G}$ we let $u(a)$ denote the smallest positive integer such that $q^{u(a)}a = a$. For every non-zero $a = (a_0, a_1, a_2, a_3) \in \widehat{G}$ we define the Jacobi sum $J(a)$ as follows: let $\chi_i : \mathbb{F}_{q^{u(a)}}^* \to \overline{\mathbb{Q}}_p$ be defined as $\chi_i = \alpha^{\frac{q^{u(a)}-1}{d} a_i}$ and set $J(a) = J(\chi_0, \ldots, \chi_3)$. Note that $J(qa) = J(a)$. By convention, we set $J(0) = q$. Let $\Gamma^\perp \subset \widehat{G}$ be the cyclic subgroup of order n generated by $(3, -6, 2, 1)$ and let

$$\widehat{G}' = \{a = (a_0, \ldots, a_3) \in \widehat{G} \mid a = 0 \text{ or } a_i \neq 0 \text{ for } i = 0, \ldots 3\}.$$

As in Notation 6.6 for every $\mathrm{Spec}(\mathbb{F}_q)$-scheme S let $\overline{S}$ denote again its base change to $\mathrm{Spec}(\overline{\mathbb{F}}_p)$ and let $F : \overline{S} \to \overline{S}$ denote the Frobenius relative to $\mathbb{F}_q$ for every such S. Choose a prime $l \neq p$ and fix an isomorphism $\nu : \overline{\mathbb{Q}}_l \to \overline{\mathbb{Q}}_p$. We will identify $\overline{\mathbb{Q}}_l$ with $\overline{\mathbb{Q}}_p$ via ν.

Theorem 8.8. *Let $A_1, \dots, A_k$ be the orbits of multiplication by q on $\Gamma^{\perp} \cap \widehat{G}'$ and choose $a_i \in A_i$. Then*

$$\det\Big(1 - F^*\,t | H^2(\overline{F_n/\Gamma}, \overline{\mathbb{Q}}_l)\Big) = \prod_{i=1}^{k}(1 - J(a_i)t^{u(a_i)}).$$

Proof. This is Corollary 7.7 of [29] on page 310. □

Definition 8.9. As in Notation 3.1 pick an isomorphism $\iota : \overline{\mathbb{Q}}_l \to \mathbb{C}$ and identify $\overline{\mathbb{Q}}_l$ with $\mathbb{C}$ via ι in all that follows. Let $|\cdot|_\infty$ denote the usual archimedean absolute value on $\mathbb{C}$. For every $\alpha \in \mathbb{R}$, finite dimensional $\overline{\mathbb{Q}}_l$-vector space V and $\overline{\mathbb{Q}}_l$-linear endomorphism $\Psi : V \to V$ we say that the pair (V, Ψ) has weights $\leq \alpha$ if for every eigenvalue λ of Ψ we have $|\lambda|_\infty \leq |q|^\alpha$. Moreover we say that (V, Ψ) has slope α if for every λ as above $v_q(\lambda) = \alpha$. For every $\alpha \in \mathbb{R}$, $k \in \mathbb{N}$ and scheme X of finite type over $\mathrm{Spec}(\mathbb{F}_q)$ we say that X has weights $\leq \alpha$ in dimension k if the pair $(H^k(\overline{X}, \overline{\mathbb{Q}}_l), F^*)$ has weights $\leq \alpha$. Similarly we say that X has slope α in dimension k if the pair $(H^k(\overline{X}, \overline{\mathbb{Q}}_l), F^*)$ has slope α.

Now let C be a curve over $\mathbb{F}_q$, i.e. a one-dimensional (but necessarily equidimensional) variety defined over $\mathbb{F}_q$.

Lemma 8.10. *The following holds:*

- (i) *the curve C has weights ≤ 1 in dimension 1,*
- (ii) *the curve C has slope 1 in dimension 2.*

Proof. Let U be a smooth dense open subscheme of C and let $i : U \to C$ be the inclusion map. Let S be the reduced closed subscheme of C whose underlying set is the complement of U and let $j : S \to C$ be the inclusion map. Then there is a cohomological long exact sequence:

$$\begin{tikzcd}
H^1(\overline{C}, i_!(\overline{\mathbb{Q}}_l)) \arrow[r, "\alpha"] & H^1(\overline{C}, \overline{\mathbb{Q}}_l) \arrow[r] & H^1(\overline{C}, j_*(\overline{\mathbb{Q}}_l)) \arrow[r] & \cdots \\
\cdots \arrow[r] & H^2(\overline{C}, i_!(\overline{\mathbb{Q}}_l)) \arrow[r, "\beta"] & H^2(\overline{C}, \overline{\mathbb{Q}}_l) \arrow[r] & H^2(\overline{C}, j_*(\overline{\mathbb{Q}}_l)).
\end{tikzcd}$$

Because $j_*(\mathbb{Q}_l)$ is the direct sum of skyskaper sheaves, it is acyclic. Hence the map α is surjective and the map β is an isomorphism. By the proper base change theorem $H^1_c(\overline{U}, \overline{\mathbb{Q}}_l) = H^1(\overline{C}, i_!(\overline{\mathbb{Q}}_l))$ so the pair $(H^1(\overline{C}, i_!(\overline{\mathbb{Q}}_l)), F^*)$ has weights ≤ 1 by Deligne's purity theorem. Similarly $H^2_c(\overline{U}, \overline{\mathbb{Q}}_l) = H^2(\overline{C}, i_!(\overline{\mathbb{Q}}_l))$ so the pair $(H^2(\overline{C}, i_!(\overline{\mathbb{Q}}_l), F^*)$ has slope 1 by the duality theorem. Because the maps α and β are F^*-equivariant the claims are now clear. □

Notation 8.11. Now let X be a surface over $\mathbb{F}_q$, i.e. a two-dimensional variety defined over $\mathbb{F}_q$. Let U be a smooth dense open sub-scheme of X and let $i : U \to X$ be the inclusion map. Then we have a map:

$$i_* : H^2_c(\overline{U}, \overline{\mathbb{Q}}_l) \longrightarrow H^2(\overline{X}, \overline{\mathbb{Q}}_l)$$

which is the composition of the isomorphism $H^2_c(\overline{U}, \overline{\mathbb{Q}}_l) = H^2(\overline{X}, i_!(\overline{\mathbb{Q}}_l))$ furnished by proper base change and the homomorphism $H^2(\overline{X}, i_!(\overline{\mathbb{Q}}_l)) \to H^2(\overline{X}, \overline{\mathbb{Q}}_l)$ induced by the inclusion $i_!(\overline{\mathbb{Q}}_l) \subseteq \overline{\mathbb{Q}}_l$.

Lemma 8.12. *The following holds:*

- (i) *the pair $(\mathrm{Ker}(i_*), F^*)$ has weights ≤ 1,*
- (ii) *the pair $(\mathrm{Coker}(i_*), F^*)$ has slope 1.*

Proof. Let C be the reduced closed subscheme whose underlying set is the complement of U and let $j : C \to X$ be the inclusion map. Then C is a curve and there is a cohomological long exact sequence:

$$H^1(\overline{X}, j_*(\overline{\mathbb{Q}}_l)) \to H^2(\overline{X}, i_!(\overline{\mathbb{Q}}_l)) \to H^2(\overline{X}, \overline{\mathbb{Q}}_l) \to H^2(\overline{X}, j_*(\overline{\mathbb{Q}}_l)).$$

Because $H^1(\overline{X}, j_*(\overline{\mathbb{Q}}_l)) = H^1(\overline{C}, \overline{\mathbb{Q}}_l)$ and $H^2(\overline{X}, j_*(\overline{\mathbb{Q}}_l)) = H^2(\overline{C}, \overline{\mathbb{Q}}_l)$, the pair $(H^1(\overline{X}, j_*(\overline{\mathbb{Q}}_l)), F^*)$ has weights ≤ 1 and the pair $(H^2(\overline{X}, j_*(\overline{\mathbb{Q}}_l)), F^*)$ has slope 1 by Lemma 8.10. The claims are now clear. □

Proposition 8.13. *Let X_1 and X_2 be two birationally equivalent geometrically irreducible projective surfaces over* $\mathrm{Spec}(\mathbb{F}_q)$*. Assume that both X_1 and X_2 are pure of weight* 2 *in dimension* 2*. Then*

$$l_q(\det\left(1 - F^*\, t | H^2(\overline{X}_1, \overline{\mathbb{Q}}_l)\right)) = l_q(\det\left(1 - F^*\, t | H^2(\overline{X}_2, \overline{\mathbb{Q}}_l)\right)).$$

Proof. Let U be a smooth, two-dimensional scheme over $\mathrm{Spec}(\mathbb{F}_q)$ such that there are open immersions $i_1 : U \to X_1$ and $i_2 : U \to X_1$. Then

$$l_q(\det\left(1 - F^*\, t | \mathrm{Im}(i_{k*})\right) = l_q(\det\left(1 - F^*\, t | H^2(\overline{X}_k, \overline{\mathbb{Q}}_l)\right))$$

for $k = 1, 2$, using the notation of 8.11, by part (ii) of Lemma 8.12. Let V denote the largest F^*-invariant $\overline{\mathbb{Q}}_l$-linear subspace of $H^2_c(\overline{U}, \overline{\mathbb{Q}}_l)$ which has weights ≤ 1. Because $H^2(\overline{X}_k, \overline{\mathbb{Q}}_l)$ is pure of weight 2 we have $V \subseteq \mathrm{Ker}(i_{k*})$ for $k = 1, 2$. But $V \supseteq \mathrm{Ker}(i_{k*})$ by part (i) of Lemma 8.12. Hence

$$\det\left(1 - F^*\, t | \mathrm{Im}(i_{1*})\right) = \det\left(1 - F^*\, t | H^2_c(\overline{U}, \overline{\mathbb{Q}}_l)/V\right) = \det\left(1 - F^*\, t | \mathrm{Im}(i_{2*})\right),$$

so the claim is clear. □

Assume now that $q = p$.

Theorem 8.14. *Let p be a prime number and let n be a positive integer as above. Assume that $n|p-1$ and $6|n$. Then E_n is not isotrivial and*

$$m(E_n) = \frac{n}{6} - 1 = \frac{1}{12}\deg(\Delta_{E_n}) - 1.$$

Proof. Let $\underline{a} = (-3, 6, -2, -1) \in \widehat{G}$. By our assumption for every $k = 0, 1, \ldots, n-1$ we have $k\underline{a} \in \widehat{G}'$ if and only if $k \neq n/6, n/3, n/2, 2n/3$ or $5n/6$. Because of our assumption $n|p-1$ every orbit of multiplication by p on $\Gamma^\perp \cap \widehat{G}'$ consists of one element. Hence

$$\det\left(1 - F^*\, t | H^2(\overline{F_n/\Gamma}, \overline{\mathbb{Q}}_l)\right) = \prod_{\substack{0 \leq k \leq n-1 \\ k \neq n/6, n/3, n/2, 2n/3, 5n/6}} (1 - J(k\underline{a})t) \tag{8.14.1}$$

by Theorem 8.8. Gauss sums are Weil numbers of weight 1 hence the reciprocal roots of the polynomial in (8.14.1) above are Weil numbers of weight 2. The surface $\mathcal{E}_n$ is smooth, so it is pure of weight 2 in dimension 2 by Deligne's purity theorem. Hence by Theorem 8.3 and Proposition 8.13 we have:

$$l_q(L(E_n, t)) = l_q(\det\left(1 - F^*\, t | H^2(\overline{\mathcal{E}_n}, \overline{\mathbb{Q}}_l)\right)) = l_q(\det\left(1 - F^*\, t | H^2(\overline{F_n/\Gamma}, \overline{\mathbb{Q}}_l)\right)).$$

For every $k = 1, 2, \ldots, n/6 - 1$ we have:

$$\begin{aligned} v_p(J(k\underline{a})) &= v_p\Big(g(\alpha^{\frac{-3k(p-1)}{n}}, \psi) g(\alpha^{\frac{6k(p-1)}{n} - p + 1}, \psi) g(\alpha^{\frac{-2k(p-1)}{n}}, \psi) g(\alpha^{\frac{-k(p-1)}{n}}, \psi)\Big) - 1 \\ &= \frac{3k}{n} + 1 - \frac{6k}{n} + \frac{2k}{n} + \frac{k}{n} - 1 = 0 \end{aligned}$$

by Stickelberger's Theorem 8.6, since every exponent of α^{-1} in the equation above is a positive integer strictly less than p. Hence by Proposition 4.5 and the above:

$$m(E_n) \geq l_q(L(E_n,t)) \geq \frac{n}{6} - 1.$$

Because $6|p-1$ by our assumptions, we have $p \geq 7$. Hence

$$m(E_n) \leq \frac{1}{12}\deg(\Delta_{E_n}) - 1 = \frac{n}{6} - 1$$

by Theorem 6.9 and by our remark at the end of Definition 8.1. The claim of the theorem above is now clear. □

9. Strong Weil curves

Definition 9.1. Fix now a closed point ∞ of $\mathcal{C}$ and let A denote the ring of rational functions on $\mathcal{C}$ regular away from ∞ as in the introduction. For any non-zero ideal $\mathfrak{m}$ of A an irreducible affine algebraic curve $Y_0(\mathfrak{m})$ is defined over F, the Drinfeld modular curve parameterising Drinfeld A-modules of rank two of generic characteristic with Hecke level $\mathfrak{m}$-structure. There is a unique non-singular projective curve $X_0(\mathfrak{m})$ over F which contains $Y_0(\mathfrak{m})$ as a dense open subvariety. Let $J_0(\mathfrak{m})$ denote the Jacobian of the curve $X_0(\mathfrak{m})$. The ideals of A and the effective divisors on $\mathcal{C}$ whose support does not contain ∞ are in a natural one to one correspondence, and we will not distinguish them in all that follows. Let E be an elliptic curve defined over F which has split multiplicative reduction at ∞. Then its conductor is of the form $\mathfrak{m}\infty$, where $\mathfrak{m}$ is an ideal of A. By the function field analogue of the Taniyama-Weil conjecture there is a non-constant map $\pi : X_0(\mathfrak{m}) \to E$ defined over F. For any map $h : X_0(\mathfrak{m}) \to C$, where C is an elliptic curve, let $h_* : J_0(\mathfrak{m}) \to C$ and $h^* : C \to J_0(\mathfrak{m})$ denote the maps induced by the Albanese and the Picard functoriality, respectively.

Theorem 9.2. *The following are equivalent:*

- (i) *the kernel of the map* $\pi_* : J_0(\mathfrak{m}) \to E$ *is an abelian variety,*
- (ii) *the map* $\pi^* : E \to J_0(\mathfrak{m})$ *is a closed immersion,*
- (iii) *the degree of* π *is minimal among all non-degenerate maps* $\rho : X_0(\mathfrak{m}) \to E'$*, where* E' *is any elliptic curve isogeneous to* E *over* F*.*

Proof. This result is well known in the mathematical folklore, but it is difficult to track down a proof (the standard reference, Lemme 3 of [15] on pages 282-283 only shows the equivalence of (i) and (iii)). Our excuse for giving a full proof other than the above is that we consider the more delicate case of positive characteristic. First assume that (i) holds. By the multiplicity one theorem for the action of the Hecke algebra on $J_0(\mathfrak{m})$ the abelian variety $\mathrm{Ker}(\pi_*)$ has no quotient isogeneous to E, so for every non-degenerate map $\rho : X_0(\mathfrak{m}) \to E'$, where E' is any elliptic curve isogeneous to E over F, the kernel of ρ_* must contain $\mathrm{Ker}(\pi_*)$. Hence the map ρ factors through π, in particular its degree is at least as big as the degree of π. On the other hand if (iii) holds then $\mathrm{Ker}(\pi_*)$ contains the reduction of the connected component of its identity element as a closed subgroup-scheme. The quotient E' of $J_0(\mathfrak{m})$ by the latter is an elliptic curve isogeneous to E, hence the degree the corresponding map $\rho : X_0(\mathfrak{m}) \to E'$ is at least as big as $\deg(\pi)$. But π factors through ρ, so they must be equal. Note that the map π^* is just the dual of the morphism $\pi_* : J_0(\mathfrak{m}) \to E$ of the principally polarised abelian varieties. The equivalence of (i) and (ii) and therefore the theorem itself now follows from the lemma below. □

Lemma 9.3. *Let $\phi : A \to B$ be a surjective homomorphism of abelian varieties and let $\phi^\vee : B^\vee \to A^\vee$ be its dual. Then the following are equivalent:*

(i) *the kernel of ϕ is an abelian variety,*

(ii) *the map $\phi^\vee$ is a closed immersion.*

Proof. This proof was explained to me by Laurent Fargues. For any S-scheme T let T also denote the sheaf represented by T on the *fppf* topology on S. Attached to the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Ker}(\phi) \arrow[r] & A \arrow[r, "\phi"] & B \arrow[r] & 0 \end{tikzcd}$$

of sheaves on the *fppf* topology there is a cohomological exact sequence:

$$\mathrm{Hom}(A, \mathbb{G}_m) \to \mathrm{Hom}(\mathrm{Ker}(\phi), \mathbb{G}_m) \longrightarrow \mathrm{Ext}^1(B, \mathbb{G}_m) \xrightarrow{\phi^\vee} \mathrm{Ext}^1(A, \mathbb{G}_m).$$

By a theorem of Grothendieck for any abelian scheme C the sheaf $\mathrm{Ext}^1(C, \mathbb{G}_m)$ is represented by the dual of C and for any morphism $\phi : A \to B$ of abelian varieties the induced map $\mathrm{Ext}^1(B, \mathbb{G}_m) \to \mathrm{Ext}^1(A, \mathbb{G}_m)$ is the dual of ϕ as the notation above indicates. Moreover the sheaf $\mathrm{Hom}(C, \mathbb{G}_m)$ is trivial for any abelian scheme C hence $\phi^\vee$ is an immersion if and only if $\mathrm{Hom}(\mathrm{Ker}(\phi), \mathbb{G}_m)$ is trivial. Let $\mathrm{Ker}(\phi)_0$ denote the reduced group scheme associated to the connected component of $\mathrm{Ker}(\phi)$, considered as a closed subgroup-scheme. It is an abelian subscheme of $\mathrm{Ker}(\phi)$ such that the quotient $G = \mathrm{Ker}(\phi)/\mathrm{Ker}(\phi)_0$ is a finite, flat group scheme. By looking at the cohomological exact sequence attached to the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Ker}(\phi)_0 \arrow[r] & \mathrm{Ker}(\phi) \arrow[r] & G \arrow[r] & 0 \end{tikzcd}$$

of sheaves on the *fppf* topology, we get that $\mathrm{Hom}(\mathrm{Ker}(\phi), \mathbb{G}_m) = \mathrm{Hom}(G, \mathbb{G}_m)$. The sheaf $\mathrm{Hom}(G, \mathbb{G}_m)$ is represented by the Cartier dual of the group scheme G, so it is trivial if and only if G is trivial. □

Definition 9.4. If the equivalent conditions of the theorem above hold then we say that E is a strong Weil curve and the modular parameterisation $\pi : X_0(\mathfrak{m}) \to E$ is optimal. By the proof above it is clear that up to isomorphism E is unique in its isogeny class and there is only one strong Weil map parameterising E. On the other hand by property (i) the quotient of $J_0(\mathfrak{m})$ by the reduced group scheme associated to the connected component of the kernel of the map $\pi_* : J_0(\mathfrak{m}) \to E$ induced by any modular parameterisation $\pi : X_0(\mathfrak{m}) \to E$ is a strong Weil curve. Hence there is a strong Weil curve in the isogeny class of every elliptic curve having split multiplicative reduction at ∞.

10. Applications to the degree conjecture

Definition 10.1. For any graph G let $\mathcal{V}(G)$ and $\mathcal{E}(G)$ denote its set of vertices and edges, respectively. Let R be a commutative group and let G be a locally finite oriented graph. In this paper we will assume that every oriented graph G is equipped with an involution $\bar{\cdot} : \mathcal{E}(G) \to \mathcal{E}(G)$ such that for each edge $e \in \mathcal{E}(G)$ the original and terminal vertices of the edge $\overline{e} \in \mathcal{E}(G)$ are the terminal and original vertices of e, respectively. The edge $\overline{e}$ is called the edge e with reversed orientation. If for each edge $e \in \mathcal{E}(G)$ there is exactly one edge $\overline{e} \in \mathcal{E}(G)$ whose original and terminal vertices are the terminal and original vertices of e then there is a unique involution of this type. The Bruhat-Tits tree $\mathcal{T}$ is such a graph. A function $\phi : \mathcal{E}(G) \to R$ is called a harmonic R-valued cochain, if it satisfies the following conditions:

(i) We have:

$$\phi(e) + \phi(\overline{e}) = 0 \ (\forall e \in \mathcal{E}(G)).$$

(ii) If for an edge e we introduce the notation $o(e)$ and $t(e)$ for its original and terminal vertex respectively,

$$\sum_{\substack{e \in \mathcal{E}(G) \\ o(e)=v}} \phi(e) = 0 \ (\forall v \in \mathcal{V}(G)).$$

We denote by $H(G, R)$ the group of R-valued harmonic cochains on G.

Definition 10.2. Let $Y \subset F^2$ be an A-lattice, that is, a projective A-submodule of rank two. Let $\Gamma(Y)$ denote the F-linear automorphisms of F^2 leaving Y invariant and for every ideal $\mathfrak{a} \lhd A$ let $\Gamma(Y, \mathfrak{a}) \leq \Gamma(Y)$ denote the subgroup of those elements who induce the identity on the quotient A-module $Y/\mathfrak{a}Y$. We say that a subgroup Γ of $GL_2(F)$ is arithmetic if there is an A-lattice Y and an ideal $\mathfrak{a}$ such that Γ is contained in $\Gamma(Y)$ and it contains $\Gamma(Y, \mathfrak{a})$. Let Γ be an arithmetic subgroup of $GL_2(F)$ and let F_∞ denote the completion of F with respect to the valuation corresponding to ∞. As a subgroup of $GL_2(F_\infty)$ the arithmetic group Γ acts on the Bruhat-Tits tree associated to $PGL_2(F_\infty)$ on the left, which we will denote by $\mathcal{T}$. For any abelian group M let $H_!(\mathcal{T}, M)^\Gamma$ denote the group of those Γ-invariant, M-valued harmonic cochains on $\mathcal{T}$ which has finite support as a function on the edges of the quotient graph $\Gamma \backslash \mathcal{T}$.

Definition 10.3. Next we are going to define the first homology group $H_1(\Gamma \backslash \mathcal{T}, \mathbb{Z})$. The latter has several descriptions. It may be defined as the first topological homology group of the CW-complex attached to $\Gamma \backslash \mathcal{T}$ with integral coefficients. It is also canonically isomorphic to the abelianization of the quotient $\Gamma^* = \Gamma/\Gamma_f$, where Γ_f be the normal subgroup of Γ generated by the elements of finite order. We will use a third, purely combinatorial description, since it is the most convenient for our purposes. Recall that a path on an oriented graph G is a sequence of edges $e_1, e_2, \ldots, e_n \in \mathcal{E}(G)$ such that $t(e_i) = o(e_{i+1})$ for $i = 1, 2, \ldots, n-1$. The path is closed if the equality $t(e_n) = o(e_1)$ holds, too. For each edge $e \in \mathcal{E}(G)$ let $i_e : \mathcal{E}(G) \to \mathbb{Z}$ denote the unique function such that

$$i_e(f) = \begin{cases} +1, & \text{if } f = e, \\ -1, & \text{if } f = \overline{e}, \\ \ \ 0, & \text{otherwise.} \end{cases}$$

To any closed path $e_1, e_2, \ldots, e_n$ we associate the function $\sum_{i=1}^n i_{e_i}$. We define $H_1(G, \mathbb{Z})$ as the abelian group of $\mathbb{Z}$-valued functions on $\mathcal{E}(G)$ generated by these functions. Let us return to the special case $G = \Gamma \backslash \mathcal{T}$. Let $z(\Gamma)$ denote the cardinality of the center of Γ and let Γ_e be the stabiliser of the edge $e \in \mathcal{E}(\mathcal{T})$ in Γ. Let us recall rapidly why Γ_e is finite. Let $v : GL_2(F_\infty) \to \mathbb{Z}$ the composition of the determinant and the valuation, and let $GL_2(F_\infty)_0$ denote its kernel. We claim that every arithmetic group Γ lies in $GL_2(F_\infty)_0$. Clearly it is enough to show this for $\Gamma(Y)$. The localisation of Y at each prime of A is a free module of rank two, so the determinant of every element of $\Gamma(Y)$ is a unit at each prime of A, so it is in fact a unit of A. The latter are constants, so they have valuation zero. On the other hand the stabilizator of e in $GL_2(F_\infty)_0$ is compact, so Γ_e is finite as the intersection of a compact and a discrete group. We define

$$j_\Gamma : H_1(\Gamma\backslash\mathcal{T},\mathbb{Z}) \to H_!(\mathcal{T},\mathbb{Z})^\Gamma,$$

as the map $\phi \mapsto \phi^*$ given by the rule $\phi^*(e) = |\Gamma_e|\phi(\widetilde{e})/z(\Gamma)$, where $\widetilde{e}$ is the image of the edge e in $\mathcal{E}(\Gamma\backslash\mathcal{T})$. It is easy to see that the homomorphism is well-defined, that is ϕ^* is indeed a harmonic cochain.

Proposition 10.4. *The homomorphism is j_Γ is injective with finite cokernel of exponent dividing $q^{\deg(\infty)} - 1$.*

Proof. The injectivity is trivial if the definition above is employed. Gekeler and Reversat proved that the cokernel has index prime to the characteristic p (see Proposition 6.4.4 of [5], pages 73-74). A careful reading of the proof of Lemma 3.3.3 of [5], pages 50-51, reveals that our proposition above has already been proved there, if one also uses the result quoted above. Here we reproduce their argument for the sake of the reader. Let T be a maximal tree in the connected graph $\Gamma\backslash\mathcal{T}$: the former exists by the Zorn lemma. By Serre's structure theorem the graph $\Gamma\backslash\mathcal{T}$ is the union of a finite graph and finitely many ends, hence the complement $\mathcal{E}(\Gamma\backslash\mathcal{T}) - \mathcal{E}(T)$ is finite. Let $R = \{\widetilde{e}_1, \ldots, \widetilde{e}_g\}$ be a set of representatives of $\mathcal{E}(\Gamma\backslash\mathcal{T}) - \mathcal{E}(T)$ modulo orientation, that is for every edge $e \in \mathcal{E}(\Gamma\backslash\mathcal{T}) - \mathcal{E}(T)$ exactly one of the edges e and $\overline{e}$ is listed in R. For each edge $\widetilde{e}_i \in R$ let c_i denote a closed path consisting of $\widetilde{e}_i$ and a path connecting $t(e_i)$ with $o(e_i)$ in T. For any $\phi \in H_!(\mathcal{T},\mathbb{Z})^\Gamma$ the function

$$\phi - \sum_{i=1}^{g} \frac{\phi(e_i)z(\Gamma)}{|\Gamma_{e_i}|} j_\Gamma(c_i)$$

vanishes identically outside of the maximal tree T, hence vanishes everywhere. Therefore the cokernel of j_Γ is annihilated by the smallest common multiple of the natural numbers $|\Gamma_{e_i}|/z(\Gamma)$. Since the torsion of the stabiliser of any edge $e \in \mathcal{E}(\mathcal{T})$ in the image of $GL_2(F_\infty)_0$ in $PGL_2(F_\infty)$ modulo its p-torsion group is a group of order $q^{\deg(\infty)} - 1$, the claim is now clear. □

Notation 10.5. In the rest of the paper we assume that E is a strong Weil curve and $\pi : X_0(\mathfrak{m}) \to E$ is optimal. Let Γ be the arithmetic group:

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(A) | c \in \mathfrak{m} \right\}.$$

One may associate to the strong Weil curve E an element $v_E \in H_!(\mathcal{T},\mathbb{Z})^\Gamma$ lying in the image of the map j_Γ (for its definition see 3.4 of [21] on page 3493). As it is well-known the set $\mathcal{E}(\mathcal{T})$ can be identified with $GL_2(F_\infty)/\Gamma_\infty Z(F_\infty)$ where Γ_∞ is the Iwahori subgroup:

$$\Gamma_\infty = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathcal{O}_\infty) | \infty(c) > 0 \right\}.$$

There is a natural map:

$$h : \mathcal{E}(\mathcal{T}) \to GL_2(F)\backslash GL_2(\mathbb{A})/\mathbb{K}_0(\mathfrak{m}\infty)Z(\mathbb{A})$$

which for $g \in GL_2(F_\infty)$ maps the left $\Gamma_\infty Z(F_\infty)$-coset of g to the the double coset $GL_2(F)\mathbf{g}K_0(\mathfrak{m}\infty)Z(\mathbb{A})$ of the unique element $\mathbf{g} \in GL_2(\mathbb{A})$ such that for every $x \in |\mathcal{C}|$ the x-th component of $\mathbf{g}$ is g, if x is ∞, and it is 1, otherwise. By 9.1 of [5] on page 84 the function v_E lies in the $\mathbb{Q}$-module $\mathbb{Q}(\psi_E \circ h)$ spanned by $\psi_E \circ h$. Let

$\widetilde{c}(E)$ be the unique non-negative number such that $v_E = \widetilde{c}(E)\psi_E \circ h$. By definition v_E generates the $\mathbb{Z}$-module $\mathrm{Im}(j_\Gamma) \cap \mathbb{Q}(\psi_E \circ h)$. Hence Proposition 10.4 has the following immediate

Corollary 10.6. *We have:*

$$\widetilde{c}(E) \leq (q^{\deg(\infty)} - 1)c(E)^{-1}.$$

Using the Riemann hypothesis for the L-function $L(\mathrm{Symm}^2(E), t)$ of the second symmetric square of the Galois representation $H^1(E_{\overline{F}}, \mathbb{Q}_l)$ (see Theorem 4.6 of [21] on pages 3501-3502) Papikian deduces from his main formula for the degree of modular parameterisations of elliptic curves, Proposition 1.3 of the same paper on page 3485, the following:

Theorem 10.7. *Assume that $\mathfrak{m}$ is square-free. Then we have:*

$$\deg(\pi) < \widetilde{c}(E)^2 \cdot q^{14g+\deg(\infty)+5} \cdot q^{\deg(\mathfrak{m})} \cdot \deg(\mathfrak{m})^3.$$

Combining Corollary 7.7 with Corollary 10.6 and Theorem 10.7 we get the following result:

Theorem 10.8. *Assume that p does not divide the order of $\mathrm{Pic}_0(\mathcal{C})(\mathbb{F}_q)$. Also suppose that $\mathfrak{m}$ is square-free. Then we have:*

$$\deg(\pi) < q^{18g+4\deg(\infty)+1} \cdot q^{2\deg(\mathfrak{m})} \cdot \deg(\mathfrak{m})^3.$$

References

[1] T. Chinburg, *Galois structure of de Rham cohomology of tame covers of schemes*, Ann. Math. **139** (1994), 443–490.

[2] P. Deligne, *Les constantes des équations fonctionnelles des fonctions L*, Lecture Notes in Math., vol. 349, Springer-Verlag, Berlin-Heidelberg-New York, 1973, 501–597.

[3] V. G. Drinfeld, *Elliptic modules*, [translation], Mat. Sbornik **23** (1974), 561–592.

[4] C. Faber and G. van der Geer, *Complete subvarieties of moduli spaces and the Prym map*, J. reine angew. Math. **573** (2004), 117-137.

[5] E.-U. Gekeler and M. Reversat, *Jacobians of Drinfeld modular curves*, J. reine angew. Math. **476** (1996), 27–93.

[6] D. Goldfeld and L. Szpiro, *Bounds for the order of the Tate-Shafarevich group*, Compositio Math. **97** (1995), 71–87.

[7] G. Harder, *Chevalley groups over function fields and automorphic forms*, Ann. Math. **100** (1974), 249–306.

[8] L. Illusie, *Complexe de de Rham-Witt et cohomologie crystalline*, Ann. Sci. École Norm. Sup. **12** (1979), 501–661.

[9] L. Illusie, *Ordinarité des intersections complètes générales*, The Grothendieck Festschrift, Vol. II., Progr. Math., vol. 87, Birkhauser, Boston, 1990, pp. 376–405.

[10] N. Katz, *Slope filtration of F-crystals*, Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. I, Astérisque, vol. 63, Soc. Math. France, Paris, 1979, pp. 113–163.

[11] N. Katz and W. Messing, *Some consequences of the Riemann hypothesis for varieties over finite fields*, Invent. Math. **23** (1974), 73–77.

[12] S. Lang, *Algebraic Number Theory*, Second edition, Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994.

[13] G. Laumon, *Transformation de Fourier, constantes d'équations fonctionelles et conjecture de Weil*, Publ. Math. IHES **65** (1987), 131–210.

[14] B. Mazur, *Frobenius and the Hodge filtration*, Bull. Amer. Math. Soc. **78** (1972), 653–667.

[15] B. Mazur, *Courbes elliptiques et symboles modulaires*, Séminaire Bourbaki **414** (1972), 277–294.

[16] L. Miller, *Curves with invertible Hasse-Witt-matrix*, Math. Ann. **197** (1972), 123–127.

[17] J. S. Milne, *On a conjecture of Artin and Tate*, Ann. Math. **102** (1975), 517–533.

[18] D. Mumford, *Bi-extensions of formal groups*, Algebraic Geometry, Bombay Colloquium 1968, Tata Inst. Fund. Research and Oxford Univ. Press, 1969, pp. 307–322.

[19] P. Norman and F. Oort, *Moduli of abelian varieties*, Ann. Math. **112** (1980), 413–439.

[20] M. Papikian, *Pesenti-Szpiro inequality for optimal elliptic curves*, Journal of Number Theory **114** (2005), 361–393.

[21] M. Papikian, *Analogue of the degree conjecture over function fields*, Trans. Amer. Math. Soc. **359** (2007), 3483–3503.

[22] J. Pesenti and L. Szpiro, *Inégalité du discriminant pour les pinceaux elliptiques à réductions quelconques*, Compositio Math. **120** (2000), 83–117.

[23] H.-G. Rück and U. Tipp, *Heegner points and L-series of automorphic cusp forms of Drinfeld type*, Documenta Math. **5** (2000), 365–444.

[24] W. Seiler, *Global moduli for elliptic surfaces with a section*, Compositio Math. **62** (1987), 169–185.

[25] J.-P. Serre, *Arbes, amalgames, SL_2*, Astérisque 46, third corrected edition, Société Mathematiques de France, Paris, 1983.

[26] J. H. Silverman, *Arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.

[27] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[28] K.-S. Tan, *Modular elements over function fields*, Journal of Number Theory **45** (1993), 295–311.

[29] D. Ulmer, *Elliptic curves with large rank over function fields*, Ann. Math. **155** (2002), 295–315.

[30] A. Weil, *Dirichlet series and automorphic forms*, Springer-Verlag, Berlin-Heidelberg-New York, (1971).

Department of Mathematics, 180 Queen's Gate, Imperial College, London, SW7 2AZ, United Kingdom

E-mail address: a.pal@imperial.ac.uk